(3.1.1) $$G = H + Hb + \cdots + Hb^{m-1}.$$

The equation (3.1.1) contains all possible cosets of H and these are different, since $b^i = hb^j$ with $i \neq j$ in the range from 0 to $m - 1$ would give a smaller positive power of b in H, this being either b^{i-j} or b^{j-i}. Hence $[G:H] = m$. Here m is the smallest positive power of b contained in H and also is the index of H in G. Thus, if G is infinite, since for any positive m the elements $(b^m)^r$ form a subgroup, there is a unique subgroup of index m. If G is finite, of order n, then $b^n = 1$, and so $n = mr$, and m is a divisor of n. Here, for any m dividing n, if $n = mr$ we have the elements $1, b^m, b^{2m}, \cdots, b^{(r-1)m}$ forming a subgroup of order r and index n. Since $n = mr$ can be any factorization of n into two factors, we see that there is one, and only one, subgroup of each order r dividing n.

3.2. Some Structure Theorems for Abelian Groups.

An infinite Abelian group may have a very complicated structure. As a relatively simple example, the multiplicative group of all complex numbers except zero contains elements of infinite order and also of every finite order.

If $a^n = 1$, $b^m = 1$ in an Abelian group, then $(a^{-1})^n = 1$ and $(ab)^m = 1$, whence the elements of finite order in any Abelian group A form a subgroup F. Every endomorphism α of A maps an element of finite order onto an element of finite order. Thus, in the sense of §2.4, F is a fully invariant subgroup of A. In §1.8 we introduced the term *periodic group* (the term *torsion group* is used in certain applications) for a group all of whose elements are of finite order. In contrast a group in which no element except the identity is of finite order is called an *aperiodic group* (or *torsion-free group*).

Theorem 3.2.1. *Given an Abelian group A. Let F be the subgroup of elements of finite order. Then A/F is aperiodic.*

Proof: Suppose to the contrary that $x \neq 1$ in A/F is of finite order m. Then in the homomorphism $A \to A/F$ let $u \to x$. Then $u^m \to x^m = 1$, whence $u^m \in F$ and u^m is of some finite order, say, n. Here $(u^m)^n = 1$ and u itself is of finite order. Thus $u \in F$ and $u \to 1$ although we assumed $x \neq 1$.

This theorem reduces the problem of constructing all Abelian groups to three more explicit problems:

1) The determination of all periodic Abelian groups.
2) The determination of all aperiodic Abelian groups.
3) The construction of an Abelian group A with a given periodic group F as a subgroup, such that the factor group A/F shall be isomorphic to a given aperiodic group H. No one of these is completely settled, but it appears that we know most about the first and least about the last.

We shall say that a set of elements a_i in an Abelian group A is *independent* if a finite product $\prod_i a_i^{e_i} = 1$ only when $a_i^{e_i} = 1$ for every i. If the a_i are independent and also generate A, we say that the a_i form a *basis* for A. Thus elements a_i form a basis for A if, and only if, A is the direct product of the cyclic groups generated by the a_i.

Suppose an Abelian group A is generated by elements $a_1, \cdots, a_r$. Then every element of A is of the form $a_1^{u_1} \cdots a_r^{u_r}$, where the u_i are integers. If

(3.2.1) $$a_1^{x_1} \cdots a_r^{x_r} = 1$$

is a relation on these generators, we say that

(3.2.2) $$a_1^{-x_1} \cdots a_r^{-x_r} = 1$$

is its inverse relation. From a set S of relations holding in A we may derive others by taking the product of relations of S and inverses of relations of S. Two sets of relations S_1 and S_2 are said to be *equivalent* if the relations of each set may be derived in this way from the relations of the other set. This is easily seen to be a true equivalence. We say that a set S is a set of *defining relations* for A if every relation holding in A may be derived from those of S. It may be shown that an arbitrary set S of relations on generators $a_1, \cdots, a_r$ is a set of defining relations for that Abelian group A generated by $a_1, \cdots, a_r$ in which the relations derived from S hold, but no others hold. The group A may, of course, reduce to the identity element alone.

Theorem 3.2.2. *An Abelian group generated by a finite number r of elements has a basis of, at most, r elements.*

Proof: The theorem is trivially true for $r = 1$, since then the group is cyclic. Suppose that A is generated by $a_1, \cdots, a_r$. Our proof will be based on induction on r, and for fixed r on the smallest positive integer m such that $x_i = m$ in a relation

$$a_1^{x_1} \cdots a_r^{x_r} = 1. \tag{3.2.3}$$

If there is only the relation with all $x_i = 0$, then A is the direct product of the infinite cyclic groups $\{a_i\}$ and our theorem is true. Otherwise, some relation or its inverse will contain some positive exponents. Let us renumber the a's, if necessary, so that the smallest positive exponent in a relation is $x_1 = m$. If $m = 1$, then we have

$$a_1 = a_2^{-x_2} \cdots a_r^{-x_r}, \tag{3.2.4}$$

and A is generated by the $r - 1$ elements $a_2, \cdots, a_r$, and by induction our theorem is true. Now suppose $x_1 = m > 1$ in the relation

$$a_1^m a_2^{x_2} \cdots a_r^{x_r} = 1. \tag{3.2.5}$$

Let $y_1, \cdots, y_r$ be the exponents in a further relation. Then, for any integer k, from this relation and (3.2.5) we may derive a relation with exponents $y_1 - km$, $y_2 - kx_2, \cdots, y_r - kx_r$. We may choose k so that $0 \leq y_1 - km < m$. But since m was the smallest positive exponent in any relation, we must have $y_1 - km = 0$, and so the relation with exponents $y_1, \cdots, y_r$ can be derived from (3.2.5) and the relation with exponents $0, y_2 - kx_2, \cdots, y_r - kx_r$. Thus the set of all relations for A is equivalent to the set S consisting of (3.2.5) and relations involving only $a_2, \cdots, a_r$.

In (3.2.5) let $x_2 = k_2 m + s_2, \cdots, x_r = k_r m + s_r$, where we choose k_i, $i = 2, \cdots, r$ so that $0 \leq s_i < m$. If we take a new element

$$a_1^* = a_1 a_2^{k_2} \cdots a_r^{k_r}, \tag{3.2.6}$$

then $a_1^*, a_2, \cdots, a_r$ also generate A, and in terms of these generators, (3.2.5) becomes

$$a_1^{*m} a_2^{s_2} \cdots\cdot a_r^{s_r} = 1. \tag{3.2.7}$$

Here if any s is different from zero, it is a positive number less than m and we may apply our induction. But if $s_2 = \cdots = s_r = 0$, then (3.2.7) becomes

$$a_1^{*m} = 1, \tag{3.2.8}$$

and since (3.2.5) and relations involving only $a_2, \cdots, a_r$ were a defining set of relations for A in terms of generators $a_1, a_2, \cdots, a_r$, it follows

that (3.2.8) and relations involving only $a_2, \cdots, a_r$ are a defining set of relations in terms of generators $a_1^*, a_2, \cdots, a_r$. Hence A is the direct product of the cyclic group of order m generated by a_1^* and the group generated by the $r - 1$ elements $a_2, \cdots, a_r$, which by our induction is the direct product of, at most, $r - 1$ cyclic groups. Thus we have proved our theorem in all cases.

To study periodic Abelian groups we need a lemma which holds in any group.

LEMMA 3.2.1. *Let x be an element of order mn in any group where m and n are relatively prime integers. Then x has a unique representation $x = yz = zy$, where y is of order m and z of order n. Both y and z are powers of x.*

Proof: We write (a,b) for the greatest common divisor of two integers. The statement that m and n are relatively prime is that $(m,n) = 1$. From the Euclidean algorithm, integers u and v exist such that $um + vn = 1$, and hence $x = x^{vn}x^{um} = x^{um}x^{vn}$. Put $y = x^{vn}$, $z = x^{um}$. Then $x = yz = zy$ and $y^m = x^{vnm} = 1$, and $z^n = x^{umn} = 1$. Thus the exact order of y is some divisor m_1 of m, and of z some divisor n_1 of n. But from $x = yz = zy$ it will follow that the order of x is a divisor of $m_1 n_1$. Since this order was mn, it follows that $m_1 = m$ is the order of y and $n_1 = n$ is the order of z. If x had a second representation $x = y_1 z_1 = z_1 y_1$ with y_1 of order m and z_1 of order n, let us note first that y_1 and z_1 permute with x, since $xy_1 = y_1 z_1 y_1 = y_1 x$ and $xz_1 = z_1 y_1 z_1 = z_1 x$. But then y_1 and z_1 permute with y and z, which are powers of x. Now $yz = x = y_1 z_1$ leads to $w = y_1^{-1}y = z_1 z^{-1}$. But y and y_1 are permuting elements of order m, and z and z_1 are permuting elements of order n. Hence the element w satisfies $w^m = 1$ and also $w^n = 1$, and since $(m, n) = 1$, this yields $w = 1$; so, $y_1 = y$, $z_1 = z$, proves the uniqueness of the representation.

By repeated application of this lemma we find:

LEMMA 3.2.2. *Let x be an element of order $n = n_1 n_2 \cdots n_r$ where $(n_i, n_j) = 1$ for $i \neq j$. Then x has a unique representation $x = x_1 x_2 \cdots x_r$ where $x_j x_i = x_i x_j$ and x_i is of order n_i. Every x_i is a power of x.* In particular, if $n = p_1^{e_1} \cdots p_r^{e_r}$, where $p_1, \cdots, p_r$ are distinct primes, we may apply this lemma with $n_i = p_i^{e_i}$.

In a periodic Abelian group A consider the set of elements P whose orders are powers of a fixed prime p, where we include the identity as