Cubo Matemática Educacional
Vol. 4, Nº1, MAYO 2002

AN INTRODUCTION TO THE STRUCTURE OF ABELIAN GROUPS

David M. Arnold

Department of Mathematics, Baylor University,
Waco, TX 76798-7328/U.S.A.
e-mails: David_Arnold@baylor.edu

Abstract

The definition of an abelian group is an abstraction of familiar properties of the set of integers. Some major structural theorems for abelian groups are discussed from an elementary point of view. Numerous examples are included.

1 Introduction

Fundamental properties of the integers are encountered early in a student's mathematical education. For example finding an integer n with $7 + n = 15 + (19 + 85)$ by inspection can be accomplished by writing $7 + n = (15 + 85) + 19 = 119$ so that $n = -7 + 119 = 112$. This simple solution uses the commutative law for addition $(19+85 = 85+19)$, the associative law for addition $(15+(85+19) = (15+85)+19)$, and the existence of an additive inverse -7 of 7 $(7 + (-7) = 0)$.

The definition of an abelian group can be viewed as an abstraction of these fundamental properties. Specifically, an *abelian group* is a set G together with an operation $+$ on pairs of elements of G satisfying the following axioms:

(i) closure: $a+b$ is a unique element of G for each pair a, b of elements of G;

(ii) commutativity: $a+b=b+a$ for each pair a, b of elements of G;

(iii) associativity: $a+(b+c)=(a+b)+c$ for each triple a, b, and c of elements of G;

(iv) identity: there is an element of G, denoted by 0, such that $a+0=a=a+0$ for each element a of G;

(v) inverse: for each element a of G, there is an element of G, denoted by $-a$, such that $a+(-a)=0=(-a)+a$.

Abelian groups arise naturally in many areas of mathematics, both elementary and sophisticated. For example, the set $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, 3, ...\}$ of integers with addition as $+$ satisfy axioms (i) -(v), as does the set $\mathbb{Q} = \{a/b : a, b \in \mathbb{Z}, 0 \neq b\}$ of fractions with $+$ defined by $a/b + c/d = (ad+bc)/bd$. Notice that in the abelian group $\mathbb{Q}$, $0 = 0/a \in \mathbb{Q}$ for each $0 \neq a \in \mathbb{Q}$ and $-(\ a/b) = (-a)/b \in \mathbb{Q}$ for each $a/b \in \mathbb{Q}$. The set of real numbers $\mathbb{R}$, the set of complex numbers $\mathbb{C}$, and vector spaces over either $\mathbb{R}$ or $\mathbb{C}$, essential tools for such disciplines as engineering and physics, are all examples of abelian groups with addition as $+$ in each case. On a more advanced mathematical level, additive groups of rings and modules are abelian groups, as are homology groups, cohomology groups, and certain homotopy groups arising in algebraic topology.

Another example of an abelian group bearing a resemblance to the group $\mathbb{Z}$ of integers is $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, ..., n-1\}$ for a fixed positive integer $n > 1$. This is the set of all possible remainders obtained by dividing positive integers by n. The operation $+$ on $\mathbb{Z}/n\mathbb{Z}$, called *addition modulo n,* is given by $i+j=k$, where k is the remainder when $i+j$ is divided by n.

For example, if $n = 12$, then $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/12\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. In $\mathbb{Z}/12\mathbb{Z}$, $5+8=1$, since $5+8=12+1$ shows that the remainder is 1 when $5+8$

is divided by 12. On the other hand, $-8 = 4 \in \mathbb{Z}/12\mathbb{Z}$ because $8 + 4 = 0$ in $\mathbb{Z}/12\mathbb{Z}$ (observing that 0 is the remainder when $8 + 4$ is divided by 12). Consequently, in $\mathbb{Z}/12\mathbb{Z}$, $5 - 8 = 5 + (-8) = 5 + 4 = 9$. These calculations are familiar to clock-watchers, since if the time is now 5 o'clock, then it will be 1 o'clock in 8 hours ($5 + 8 = 1$) and the time was 9 o'clock 8 hours earlier ($5 - 8 = 9$). In this case, the arithmetic takes place in $\mathbb{Z}/12\mathbb{Z}$, since a normal clock has only twelve hours, namely $12 = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$, and 11. For a twenty-four hour clock, the arithmetic would take place in $\mathbb{Z}/24\mathbb{Z}$.

If G is an abelian group, $x \in G$, and $n \in \mathbb{Z}$ is an integer, then nx is an element of G. This is a consequence of the axioms for an abelian group because $nx = x + ... + x$ (n terms) is an element of G if $n \geq 1$, $nx = (-x) + ... + (-x) \in G$ if $n < 0$, and $0x = 0 \in G$.

A basic problem in abelian group theory is the structure problem: Can a given abelian group be identified as a combination of familiar groups? This is one of the most important problems for applications to other areas, especially in the case that an abelian group models a physical situation. Within more advanced mathematics, classification of a homology, cohomology, or homotopy group of a topological space provides information about the topological and geometric nature of the space. The commutative axiom (axiom (ii)) is essential to make the structure problem feasible for finite groups, where a *finite group* is a finite set with an operation + satisfying axioms (i), (iii), (iv), and (v) but not necessarily (ii). As discussed in Section 1, all finite abelian groups can be identified. On the other hand, the structure problem for a finite group in general is currently just too complicated to resolve.

The two terms "identified" and "combination" in the structure problem can be made more specific. As for "combination", given two abelian groups G and H, define $G \oplus H$ to be the set of ordered pairs (g, h) with $g \in G$ and $h \in H$. This set is an abelian group, where + on $G \oplus H$ is defined by $(g_1, h_1) + (g_2, h_2) = (g_1 + g_2, h_1 + h_2)$. In this case, the identity is $0 = (0, 0) \in G \oplus H$ and the inverse $-(g, h)$ of (g, h) is $(-g, -h) \in G \oplus H$. The abelian group $G \oplus H$ is called the *direct sum* of G and H and G is called a *summand* of $G \oplus H$. More generally, given abelian groups $G_1, ..., G_n$, $G_1 \oplus ... \oplus G_n = \{(g_1, ...g_n) : g_i \in G_i\}$ with + defined by $(g_1, ...g_n) + (h_1, ...h_n) = (g_1 + h_1, ..., g_n + h_n)$ is the direct sum of these groups.

For example, the elements of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ are $(0,0), (0,1), (0,2), (1,0), (1,1)$, and $(1,2)$. Let's look at some arithmetic in $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$:

$$2(1,1) = (1,1) + (1,1) = (1+1, 1+1) = (0,2),$$
$$3(1,1) = (1,1) + (1,1) + (1,1) = (1+1+1, 1+1+1) = (1,0)$$
$$4(1,1) = (0,1)$$
$$5(1,1) = (1,2), \text{ and}$$
$$6(1,1) = (0,0).$$

A quick inspection shows that the elements of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, with $x = (1,1)$, are precisely $0 = 0x, x = 1x, 2x, 3x, 4x$, and $5x$. From this perspective, + in $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ is given by $ix + jx = kx$, where $i + j = k$ is computed in $\mathbb{Z}/6\mathbb{Z}$. Consequently, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ "looks like" $\mathbb{Z}/6\mathbb{Z}$, a suspicion that will be made precise.

Two abelian groups G and H are *isomorphic* if there is a 1-1 and onto function f from G to H such that $f(a + b) = f(a) + f(b)$ for each a and b in G. In this case, f is called an *isomorphism*. For instance, $G = \mathbb{Z}/6\mathbb{Z}$ is isomorphic to $H = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, the isomorphism f being defined by $f(i) = ix$ for each $i \in \mathbb{Z}/6\mathbb{Z}$. Isomorphism is the sense in which two abelian groups are identified.

On the other hand, $\mathbb{Z}/4\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, even though both groups have four elements. To see this, first observe that $2(i,j) = 0$ for each $(i,j) \in \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. If there actually was an isomorphism f from $\mathbb{Z}/4\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then $f(0) = 0 = 2f(1) = f(1) + f(1) = f(2)$. Since $0 \neq 2 \in \mathbb{Z}/4\mathbb{Z}$, this would be a contradiction to the assumption that the function f is $1 - 1$. Thus, $\mathbb{Z}/4\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

The structure problem can now be described more precisely: Is an abelian group isomorphic to the direct sum of known groups? The questions of which groups are "known" and the extent to which direct sums are unique are discussed further in subsequent sections.

The author wishes to thank Treven Wall for reading an earlier version of this manuscript and for his helpful comments.

2 Finitely generated abelian groups

A subset $X = \{x_1, ..., x_n\}$ of an abelian group G is a *finite set of generators for* G if n is a positive integer and for every element x of G there are integers $a_1, ..., a_n$ with $x = a_1x_1 + ... + a_nx_n$. In this case, G is a *finitely generated abelian group.* A finite abelian group is finitely generated since, in this case, the entire group may be chosen to be the set of generators. A set of generators for a finite abelian group, in fact even their number, need not be unique. For example, $X = \{1\}$, $X = \{5\}$, and $X = \{2, 3\}$ are all sets of generators for $\mathbb{Z}/6\mathbb{Z}$. However, $X = \{2\}$ is not a generating set for $\mathbb{Z}/6\mathbb{Z}$ since the subset $\{n2 : n \in \mathbb{Z}\}$ of elements of $\mathbb{Z}/6\mathbb{Z}$ generated by 2 is $\{0, 2, 4\} \neq \mathbb{Z}/6\mathbb{Z}$.

An abelian group that can be generated by a single element is called a *cylic group.* A cyclic group is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some $n \geq 1$. It is consistent with the definitions to identify $\mathbb{Z}$ with $\mathbb{Z}/0\mathbb{Z}$ and the single element group $\{0\}$ with $\mathbb{Z}/1\mathbb{Z}$.

The following theorem is a good example of a structure theorem in that a finitely generated abelian group is identified, up to isomorphism, as a direct sum of cyclic groups and cyclic groups are identified, up to isomorphism, as $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some $n \geq 1$ [Gallian 98]. This theorem is attributed to L. Kronecker in 1858.

Theorem 1 *A finitely generated abelian group is a direct sum of cyclic groups.*

There are a number of proofs of the preceding theorem. Following is an outline of an old, but algorithmic, argument provided that the group is expressed in terms of generators and relations. For complete details see [Mines, Richman, Ruitenburg 88].

A finitely generated abelian group G can be represented as a finite set $X = \{x_1, ..., x_n\}$ of generators and a set of relations expressed as an $m \times n$ matrix $N = (a_{ij})_{m\times n}$ with $m \leq n$ and each a_{ij} an integer such that, for each i, $\sum\{a_{ij}x_j : 1 \leq j \leq n\} = 0$. For example, $\mathbb{Z}/6\mathbb{Z}$ can be represented either by $X = \{1\}$, $N = (6)_{1\times 1}$ or by $X = \{2, 3\}$ and N = $\begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}_{2\times 2}$. A $\mathbb{Z}$-matrix is a matrix with all entries integers and a $\mathbb{Z}$−matrix is *invertible* if its determinant is ±1.

Given an $m \times n$ $\mathbb{Z}$-matrix N, there are invertible $\mathbb{Z}$−matrices P and Q with

$$S = PNQ = \begin{pmatrix} d_1 & 0 & . & . & 0 \\ 0 & d_2 & 0 & . & 0 \\ . & . & . & . & . \\ 0 & 0 & d_{m-1} & 0 & 0 \\ 0 & . & 0 & d_m & 0 \end{pmatrix}$$

an $m \times n$ matrix consisting of integers $d_1, ..., d_m$ on the diagonal of the $m \times m$ submatrix and zeroes elsewhere, such that d_i divides d_{i+1} (evenly) for each i. The matrix S is called the *Smith normal form* of the integer matrix N derived by H. Smith in 1861. The Smith normal form of an integer matrix can be computed by modern computational software packages such as Maple. The $\mathbb{Z}$-matrix S results in a new set $Y = \{y_1, ..., y_n\}$ of generators of G with relation matrix S. It follows that G is isomorphic to the direct sum $\mathbb{Z}/d_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/d_m\mathbb{Z}$ of cyclic groups.

As an illustration of this argument suppose that the abelian group G has generators $\{x_1, x_2, x_3\}$ and relation matrix

$$N = \begin{pmatrix} 4 & 6 & 0 \\ 2 & 3 & 1 \\ 8 & 12 & 2 \end{pmatrix}.$$

Elementary invertible row operations on N (multiplication by ±1, interchanging rows, and adding an integral multiple of one row to another) correspond to multiplying N on the left by an invertible $\mathbb{Z}$-matrix P just as for elementary invertible row operations for real-valued matrices. Similarly, elementary invertible column operations on N correspond to multiplying N on the right by an invertible $\mathbb{Z}$-matrix Q.

Interchange columns of N to obtain

$$\begin{pmatrix} 0 & 4 & 6 \\ 1 & 2 & 3 \\ 2 & 8 & 12 \end{pmatrix}$$

and interchange the first and second rows of this matrix to get

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 6 \\ 2 & 8 & 12 \end{pmatrix}.$$

This sequence of operations was done to put the entry 1 of N of least non-zero absolute value into the upper left hand corner. Use an elementary row operation (multiply the first row by -2 and add to the third row) to clear the first column, thereby obtaining

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 6 \\ 0 & 4 & 6 \end{pmatrix}.$$

Subtracting the third row from the second gives

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 6 \\ 0 & 0 & 0 \end{pmatrix}.$$

Next, clear the entries of the first row by elementary invertible column operations to get

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 6 \\ 0 & 0 & 0 \end{pmatrix}.$$

So far, the process used is that of Gaussian elimination for real valued matrices. However, in this case we cannot take the next step, i.e. multiply the second column by $-6/4$ and add to the third column, because the only scalars allowed are integers. Fortunately, greatest common divisors can be used to complete the process.

The greatest common divisor of two positive integers a and b is denoted by $\gcd(a, b)$. From the second row of the preceding matrix, $\gcd(4, 6) = 2$. Moreover, $2 = (-1)4 + (1)6$ (this is a special case of the fact that if a and b are integers with $\gcd(a, b) = d$, then there are integers r and s with $d = ra + sb$). Hence,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 6 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -6/2 \\ 0 & 1 & 4/2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

with

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -6/2 \\ 0 & 1 & 4/2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -3 \\ 0 & 1 & 2 \end{pmatrix}$$

an invertible $\mathbb{Z}$-matrix, since its determinant is 1. This shows that the Smith normal form of N is $S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

Therefore, G is isomorphic to $\mathbb{Z}/1\mathbb{Z}\oplus \mathbb{Z}/2\mathbb{Z}\oplus \mathbb{Z}/0\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}\oplus \mathbb{Z}$, recalling that $\mathbb{Z}/1\mathbb{Z} = \{0\}$ is the one-element group and $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$.

The Smith normal form of an integer matrix is known to be unique. Moreover, if G is isomorphic to the direct sum $\mathbb{Z}/d_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/d_m\mathbb{Z}$ of cyclic groups with d_i dividing d_{i+1} for each i, then G has an $m \times m$ relation matrix $S = \begin{pmatrix} d_1 & 0 & ... & 0 \\ 0 & d_2 & ... & 0 \\ . & . & . & . \\ 0 & ... & d_{m-1} & 0 \\ 0 & ... & 0 & d_m \end{pmatrix}$.

Consequently, a decomposition of G into direct sums of cyclic groups $\mathbb{Z}/d_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/d_m\mathbb{Z}$ of cyclic groups with d_i dividing d_{i+1} for each i, must be unique. On the other hand, not every direct sum decomposition of G as a direct sum of cyclic groups need be of this kind.

In particular, cyclic groups can have direct sum decompositions. For example, as noted above, $\mathbb{Z}/6\mathbb{Z}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. As the next theorem illustrates, this is due to the factorization of 6 into the product of prime numbers 2 and 3.

Theorem 2 *Let $n = p_1^{e_1} ... p_m^{e_m}$ be a factorization of an integer n into powers of distinct prime numbers $p_1, ..., p_m$. Then $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to the direct sum of cyclic groups $\mathbb{Z}/p_1^{e_1}\mathbb{Z}\oplus ... \oplus \mathbb{Z}/p_m^{e_m}\mathbb{Z}$.*

Proof. Define a function f from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/p_1^{e_1}\mathbb{Z}\oplus ... \oplus \mathbb{Z}/p_m^{e_m}\mathbb{Z}$ by $f(i) = (i(\mathrm{mod}\, p_1^{e_1}), \ ... \ , i(\mathrm{mod}\, p_m^{e_m}))$ for each i $\in \mathbb{Z}/n\mathbb{Z}$, where $i(\mathrm{mod}\, p_j^{e_j}) \in \mathbb{Z}/p_j^{e_j}\mathbb{Z}$ is the remainder when i is divided by $p_j^{e_j}$. Then $f(i+j) = f(i) + f(j)$ for each $i, j \in \mathbb{Z}/n\mathbb{Z}$.

Moreover, f is $1-1$ because the primes $p_1, \ldots, p_m$ are distinct. Since $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_m^{e_m}\mathbb{Z}$ have the same number of elements, the function f is onto as an application of the pigeon-hole principle [Grimaldi 99]. This shows that f is an isomorphism. ■

The proof of Theorem 2 can be used to prove that if $n = ab$ with $\gcd(a, b) = 1$, then $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$. The hypothesis that $gcd(a, b) = 1$ is definitely necessary, recalling that $4 = 2 \times 2$ but $\mathbb{Z}/4\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. It is used in the proof to conclude that $i = j (\operatorname{mod} ab)$ given that $i = j (\operatorname{mod} a)$ and $i = j (\operatorname{mod} b)$.

Theorem 2 is popularly known as the Chinese Remainder Theorem, as the essence of this theorem is in a third century B.C. Chinese manuscript entitled "Master Sun's Mathematical Manual". This theorem appeared in the context of finding a solution to a system of congruence equations. Given an integer $n > 1$ and integers a and b, define $a \equiv b(\text{mod } n)$ if $a(mod\ n) = b(\operatorname{mod} n)$ as elements of $\mathbb{Z}/n\mathbb{Z}$, i.e. a and b have the same remainder when divided by n; equivalently $a - b$ is evenly divisible by n. An introductory survey of properties of congruences and the underlying number theory is given in [Moreira 99].

The problem is, given positive integers a and b with $gcd(a, b) = 1$, $x_1 \in \mathbb{Z}/a\mathbb{Z}$, and $x_2 \in \mathbb{Z}/b\mathbb{Z}$, to find a simultaneous solution to the congruence equations

$$x \equiv x_1 (\operatorname{mod} a)$$
$$x \equiv x_2 (\operatorname{mod} b).$$

In modern terminology, this amounts to showing that the function f from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$ given by $f(i) = (i(\operatorname{mod} a), i(\operatorname{mod} b))$ is onto. The above proof of the Chinese Remainder Theorem appeals to the pigeon-hole principle. This is an example of a pure existence proof in that there is a solution x but the proof doesn't indicate at all how to find the solution. To find the solution, write $gcd(a, b) = 1 = ra + sb$ for some integers r and s. Then $x = sbx_1 + rax_2$ is the desired solution. This is because $x(\operatorname{mod} a) = sbx_1(\operatorname{mod} a) = (1 - ra)x_1(\operatorname{mod} a) = x_1(\operatorname{mod} a)$ and, similarly

$x \equiv x_2 (\bmod b)$.

Problems involving the simultaneous solution to systems of congruence equations are scattered throughout history, including present day puzzles that one may encounter in a variety of contexts. Here is an old problem from a medevial manuscript [Ore, 48]:

"An old woman goes to market and a horse steps on her basket and crushes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she counted them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them out seven at a time they came out even. What is the smallest number of eggs she could have?"

A moments thought reveals that, since the least common multiple of 2,3,4,5, and 6 is 60, the problem is asking for a simultaneous solution to the two equations $x \equiv 1 (\bmod 60)$ and x$\equiv 0 (\bmod 7)$. The above procedure, or even trial and error by finding the smallest integer of the form $60m + 1$ that is divisible by 7, reveals that 301 is the least number of eggs that the woman could have in her basket.

There are important applications of finite groups, especially $\mathbb{Z}/12\mathbb{Z}$, to the theory of music. See [Albuquerque, Oliveira 99] for a survey of some of these applications.

Combining Theorems 1 and 2 and the fact that the direct sum decomposition of Theorem 2 is unique up to isomorphism and order of direct summands yields:

Corollary 3 *(Fundamental theorem for finitely generated abelian groups) A finitely generated abelian group is isomorphic to a finite direct sum of cyclic groups isomorphic to $\mathbb{Z}$ and cyclic groups isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for n a power of a prime. Such a decomposition is unique up to isomorphism and order of summands*

Corollary 3 results in a procedure for listing all abelian groups with a given finite number of elements. The first step is a factorization of a positive integer n as a product of powers of distinct primes, say $n = p_1^{e_1} ... p_m^{e_m}$. An abelian group with n elements must be uniquely a direct sum of m groups with $p_j^{e_j}$ elements for $1 \leq j \leq m$. Moreover, the number of groups with p^j elements, for p a prime, correspond to the number of positive integer partitions of j.

For example, the only abelian groups with $8 = 2^3$ elements, up to isomorphism, are $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, corresponding respectively to the partitions $3 = 3$, $3 = 1+2$, and $3 = 1+1+1$ of 3. No two of these three groups are isomorphic, since $4(i,j) = 0$ for each $(i,j) \in \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ and $2(i,j,k) = 0$ for each $(i,j,k) \in \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

3 Torsion and divisible abelian groups

A distinguishing feature of finite abelian groups from finitely generated abelian groups in general is that each non-zero element x of a finite abelian group G has *finite order* (i.e. there is a non-zero positive integer n with $nx = 0 \in G$). For example, the order of 1 in $\mathbb{Z}/n\mathbb{Z}$ for $n > 1$ is n, while the order of 1 in $\mathbb{Z}$ is *infinite* (not finite). An abelian group G is a *torsion group* if each non-zero element of G has finite order and *torsion-free* if each non-zero element has infinite order. In view of Corollary 3, finite abelian groups are the finitely generated abelian groups that are torsion. Furthermore, finitely generated abelian groups that are torsion free are *free groups,* i.e. groups isomorphic to direct sums of $\mathbb{Z}$.

An abelian group G is a *p-group,* for a prime p, if each non-zero element of G has order a power of p, i.e. for each $0 \neq x \in G$, there is some positive integer e with $p^e x = 0$. The following theorem reduces the study of torsion abelian groups to that of p-groups.

The notion of finite direct sums of abelian groups extends naturally to infinite direct sums of abelian groups. Let I be a set and $\{G_i : i \in I\}$ a set of abelian groups indexed by I. Define an abelian group $\oplus_{i\in I} G_i$, called the *direct sum* of $\{G_i : i \in I\}$, to be the set of sequences $(g_i)_{i\in I} \in \Pi_{i\in I} G_i$ such that $g_i = 0$ for all but finitely many $i \in I$ with + defined by $(g_i)_{i\in I} + (h_i)_{i\in I} = (g_i + h_i)_{i\in I} \in \oplus_{i\in I} G_i$.

The condition that an abelian group G is isomorphic to a direct sum of abelian groups can be expressed in terms of subgroups of G, where a non-empty subset H of G is a *subgroup* of G if $a - b \in H$ for each pair of elements a and b of H In particular, the identity element 0 of G is an element of each subgroup H of G, since if $a \in H$, then $0 = a - a \in H$.

Let $\{G_i : i \in I\}$ be a set of subgroups of an abelian group G. Then G is equal to $\oplus_{i \in I} G_i$ if and only if each element g of G can be written uniquely as $g = \sum\{g_i : i \in F\}$ for some finite subset F of I and $g_i \in G_i$. An equivalent criterion is that

(i) $G = \sum_{i \in I} G_i$ (for each $a \in G$ there is a finite subset F of I with $a = \sum_{i \in F} a_i$ and each $a_i \in G_i$) and

(ii) for each $i \in I$, $G_i \cap \sum_{i \neq j \in I} G_j = \{0\}$

For instance, $G_1 = \{0, 2, 4\}$ and $G_2 = \{0, 3\}$ are subgroups of $\mathbb{Z}/6\mathbb{Z}$ with $\mathbb{Z}/6\mathbb{Z} = G_1 \oplus G_2$. This is because each element a of $\mathbb{Z}/6\mathbb{Z}$ can be written uniquely as $a = a_1 + a_2$ for some $a_i \in G_i$.

Theorem 4 *A torsion abelian group G can be written uniquely as a direct sum of p-groups.*

Proof. For each prime p, let G_p be the set of non-zero elements of G with order a power of p. Then each G_p is a p-group and a subgroup of G. The goal is to prove that $G = \oplus_{p \in \Pi} G_p$, where Π denotes the set of prime numbers.

To see that (i) holds, i.e. $G = \sum_{p \in \Pi} G_p$, let $0 \neq a \in G$ and $n = p_1^{e_1} ... p_m^{e_m}$ the least positive integer with $na = 0$. Since the primes p_i are distinct, there are integers r_i with $1 = \sum\{r_i(n/p_i^{e_i}) : 1 \leq i \leq m\}$. Then $a = \sum\{r_i(n/p_i^{e_i})a : 1 \leq i \leq m\}$ with each $r_i(n/p_i^{e_i})a \in G_{p_i}$. As for (ii), if $p \in \Pi$, and $a \in G_p \cap \sum_{p \neq q} G_q$, then $\mathrm{p}^e a = 0 = ma$ for some integer m relatively prime to p. Writing $1 = rp^e + sm$ for some integers r and s gives $a = rp^e a + sma = 0$. Uniqueness follows from the observation that if f is an isomorphism from G to $\oplus_{p \in \Pi} H_p$ with each H_p a p-group, then f is an isomorphism from G_p to H_p for each prime p. ■

Given an abelian group G and integer n, define $nG = \{na : a \in G\}$, a subgroup of G. An abelian group G is *bounded* if there is an integer n with $nG = 0$. Clearly, a bounded abelian group must be a torsion group. The next theorem, proved by H. Prüfer in 1923 and R. Baer in 1934, is another example of a good structure theorem. The proof uses infinite set theory (Zorn's Lemma) and is not included; see [Kaplansky 69] or [Fuchs 70]. Since a finite torsion abelian group is necessarily bounded, this theorem is a generalization of Corollary 3.

Theorem 5 *A bounded abelian group is a direct sum of cyclic groups of prime power order.*

Not every direct sum of cyclic groups of prime power order is bounded. For example, given a prime p, $G = \oplus\{\mathbb{Z}/p^i\mathbb{Z} : 1 \leq i\}$ is not bounded. An abelian group G is *countable* if the set G can be put into 1-1 correspondence with the natural numbers. The pentultimate theorem of this section, proved by H. Prüfer in 1921, is a structure theorem for a large class of countable p-groups.

Theorem 6 *Let p be a prime. A countable p-group G is a direct sum of cyclic groups if and only if* $\cap\{p^iG : 1 \leq i\} = \{0\}$.

A *complex nth root of unity* for a positive integer n is a complex number z with $z^n = 1$. For example, $z = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$ is a complex nth root of unity. Given a prime p, the set of complex p^i roots of unity with $i = 1, 2, ...$ is a countable abelian p-group, denoted by $\mathbb{Z}(p^\infty)$, with + defined by multiplication of complex numbers and 1 the identity for +. An alternate, but equivalent, definition of $\mathbb{Z}(p^\infty)$ is an abelian group with generators $x_1, ..., x_n, x_{n+1}, ...$ and relations $px_1 = 0$, $px_2 = x_1, \ldots, px_{n+1} = x_n, \ldots$. Now $p^i\mathbb{Z}(p^\infty) = \mathbb{Z}(p^\infty)$ for each $1 \leq i$ and so $\cap\{p^i\mathbb{Z}(p^\infty) : 1 \leq i\} = \mathbb{Z}(p^\infty)$. In view of the preceding theorem, $\mathbb{Z}(p^\infty)$ is not a direct sum of cyclic groups.

An abelian group G is *divisible* if $nG = G$ for each non-zero integer n. Examples of divisible groups include $\mathbb{Z}(p^\infty)$ and $\mathbb{Q}$, the additive group of rational numbers. Divisible groups are identified as a consequence of the final structure theorem of this section.

Theorem 7 *A divisible abelian group is isomorphic to a direct sum of copies of* $\mathbb{Q}$ *and* $\mathbb{Z}(p^\infty)$ *for primes p.*

As an application of the preceding theorem, $\mathbb{R}$, the additive group of real numbers, is isomorphic to an uncountable direct sum of copies of $\mathbb{Q}$. In particular, $\mathbb{R}$ is a $\mathbb{Q}$-vector space with an uncountable basis. Once again, the proof is a pure existence proof, as the proof does not demonstrate how to find such a basis.

More profound properties of torsion groups are presented in [Kaplansky 69], [Griffith 70], and [Fuchs 70,73]. While the structure problem has been resolved for large classes of abelian p-groups, it is far from being resolved for abelian p-groups in general.

4 Torsion-free abelian groups

Each torsion-free abelian group G is isomorphic to a subgroup of a torsion-free divisible group. Hence, G may be realized as a subgroup of a vector space over $\mathbb{Q}$ of least dimension, called the *rank* of G. For example, the torsion-free abelian groups of rank 1 are just the subgroups of 1-dimensional $\mathbb{Q}$ -vector spaces. Up to isomorphism, these groups are just subgroups of $\mathbb{Q}$.

Subgroups of $\mathbb{Q}$ can be identified up to isomorphism by sequences of non-negative integers and ∞. For purposes of identification of a non-zero subgroup X of $\mathbb{Q}$ up to isomorphism, it is sufficient to assume that $1 \in X$. To see this, let $0 \neq m/n \in X$. Then $(m/n)X$ is a subgroup of $\mathbb{Q}$ that is isomorphic to X and contains 1.

For each prime p, let $h_p^X(1)$ be the largest non-negative integer n with $1/p^n \in X$ if such an n exists and $h_p^X(1) = \infty$ if there is no largest such n. Define $h(X)$ to be the sequence $(h_p^X(1))_{p\in\Pi}$ indexed by the set Π of all primes. It follows that X is the subgroup of $\mathbb{Q}$ generated by $\{1/p^{h_p^X(1)} : p \in \Pi\}$. For example, $h(\mathbb{Z}) = (0, ..., 0, ...)$ is the sequence of all zeros and $h(\mathbb{Q}) =(\infty, ..., \infty, ...)$ is the sequence of all ∞'s.

Conversely, define a *height sequence* $h = (h_p)_{p\in\Pi}$ to be a sequence of non-negative integers and ∞'s indexed by the set of primes. Let X be the subgroup of $\mathbb{Q}$ generated by $\{1/p^{h_p} : p \in \Pi\}$. Then $h(X) = h$. Consequently, there is a 1-1 correspondence between subgroups of $\mathbb{Q}$ containing 1 and height sequences.

It remains to determine precisely, in terms of height sequences, when two subgroups X and Y of $\mathbb{Q}$ containing 1 are isomorphic. The groups X and Y are isomorphic if and only if there are non-zero positive integers m and n with $mX = nY$. This is because an isomorphism from X to Y is given by a function $f(x) = (m/n)x$ for some non-zero $m/n \in \mathbb{Q}$. Moreover, there are non-zero positive integers m and n with $mX = nY$ if and only if the sequences $h(X)$ and $h(Y)$ differ in at most finitely many finite entries; in other words $h_p^X(1) = h_p^Y(1)$ for all but a finite number of primes p and if $h_p^X(1) \neq h_p^Y(1)$, then both $h_p^X(1)$ and $h_p^Y(1)$ must be finite. This proves the following theorem, the sense in which torsion-free abelian groups of rank 1 can be regarded as known. This result dates back to F. Levi in 1917.

Theorem 8 *Each torsion-free abelian group X of rank 1 corresponds to a height sequence $h(X)$ of non-negative integers and ∞'s indexed by the set of primes. Moreover, X and Y are isomorphic if and only if $h(X)$ and $h(Y)$ differ in at most finitely many finite entries.*

A direct sum of torsion-free abelian groups of rank 1 is called a *completely decomposable* group. Part (a) of the next theorem is a result by R. Baer in 1937 and (b) is known as the Baer-Kulikov-Kaplansky theorem, see [Fuchs 73].

Theorem 9

(a) A completely decomposable group is uniquely a direct sum of torsion-free abelian groups of rank 1.

(b) If G is a completely decomposable group isomorphic to a direct sum $H \oplus K$ of abelian groups, then H and K are also completely decomposable groups.

While torsion-free abelian groups of rank 1 are well understood, torsion-free abelian groups of rank ≥ 2 are extremely complicated and not at all understood, see [Fuchs 73] and [Arnold 82]. This difficulty in the structure problem for torsion-free abelian groups of finite rank has been addressed by consideration of restricted classes of these groups. A natural candidate is a class of groups known as Butler groups in honor of a seminal paper by M.C.R. Butler in 1965.

A *Butler* group is a torsion-free abelian group that is generated by finitely many rank-1 subgroups, i.e. there are finitely many rank-1 subgroups $X_1, ..., X_n$ of G with $G = X_1 + ... + X_n$. This is a natural extension of the notion of a finitely generated abelian group, recalling that a finitely generated torsion-free abelian group is free.

The starting point for the extensive theory of Butler groups (see [Arnold 00]) is the following theorem. A subgroup H of a torsion-free abelian group G is a *pure subgroup* of G if $nH = H \cap nG$ for each non-zero positive integer n.

Theorem 10 *A finite rank torsion-free abelian group G is a Butler group if and only if G is a pure subgroup of a finite rank completely decomposable group.*

A special class of Butler groups is the class of *almost completely decomposable* groups, those torsion-free abelian groups of finite rank that contain a completely decomposable group as a subgroup of finite index. A relatively elementary development of known properties of almost completely decomposable groups may be found in [Mader 00]. The theories of Butler groups and almost completely decomposable groups are not at all complete, there are a substantial number of open questions, including structural questions.

5 Mixed abelian groups

A *mixed abelian group* is an abelian group that is neither torsion nor torsion-free. In this case, there must be both non-zero elements of finite order and non-zero elements of infinite order. For example, given a prime p, the infinite product $\Pi\{\mathbb{Z}/p^i\mathbb{Z} : 1 \leq i\}$ consisting of sequences $(x_1, ..., x_n, ...)$ with $x_i \in \mathbb{Z}/p^i\mathbb{Z}$ is a mixed group, since elements of the form $(0, ..., 0, 1, 0, ...)$ with exactly one non-zero entry have finite order while the element $(1, ..., 1, ...)$ with all entries 1 is an element of infinite order. Given an abelian group G, define the *torsion subgroup* $t(G)$ of G to be $\{a \in G : a$ has finite order$\}$. Then $t(G)$ is a torsion group and the factor group $G/t(G)$ is a torsion-free group, where $G/t(G) = \{a + t(G) : a \in G\}$ is the set of cosets of $t(G)$ in G with $+$ in $G/t(G)$ defined by $(a + t(G)) + (b + t(G)) = (a + b) + t(G)$.

One of the first steps in an investigation of mixed groups is the case that the mixed group really isn't mixed in the sense that $t(G)$ is a summand of G, i.e.

$G = t(G) \oplus H$ for some torsion-free subgroup H of G. The following theorem is due to R. Baer in 1936 and S.V. Fomin in 1937, see [Fuchs 73]. The abelian groups that arise in this theorem are identified in Section 3.

Theorem 11 *Let T be a torsion abelian group. Then $G = t(G) \oplus H$ for each abelian group G with $t(G)$ isomorphic to T if and only if T is a direct sum of a divisible group and a bounded group.*

A problem, posed originally by R. Baer, that is complementary to that of the previous theorem is resolved in [Griffith 70].

Theorem 12 *Let A be a torsion-free abelian group. Then $G = t(G) \oplus H$ for each abelian group G with $G/t(G)$ isomorphic to A if and only if A is a free group.*

Not much progress has been made on the structure problem for mixed abelian groups with the notable exception of those mixed groups G with $G/t(G)$ a torsion-free group of rank 1, see [Fuchs 73] and references.

A class of mixed groups for which the structure problem has been resolved is the class of *algebraically compact* groups, those abelian groups G such that whenever G is a pure subgroup of an abelian group H, then G is a summand of H.

Theorem 13 *An abelian group G is algebraically compact if and only if G is a summand of a direct product of abelian groups of the form $\mathbb{Z}/p^i\mathbb{Z}$ and $\mathbb{Z}(p^\infty)$.*

There is more to the story of algebraically compact groups. Specifically, G is algebraically compact with no divisible subgroups if and only if G is complete in the *$Z-$adic topology* on G (the topology with open sets $a + nG$ with $a \in G$ and n a non-zero integer). Moreover, these groups can be identified up to isomorphism in terms of known groups, see [Fuchs 70].

This article represents a very small sample of the known structural results for abelian groups. The structure theorem for finitely generated abelian groups (Corollary 3) is standard fare for any introductory abstract algebra textbook, e.g. [Gallian 98], but the algorithmic proof outlined in Section 2 is not the standard proof. More advanced books on the subject include [Kaplansky 69], [Griffith 70], [Fuchs 70, 73], [Mader 00], and [Arnold 82, 00]. The interested reader is encouraged to consult any of these books, and accompanying references to published research articles, for other aspects of the subject.

REFERENCES

[Albuquerque, Oliveira 99] **Albuquerque, H. and Oliveira, J.P.P.**, *Sobre a teoria de grupos em música*, Cubo Matemática Educacional, 1, 53-67, 1999.

[Arnold 82] **Arnold, D.M.**, *Finite Torsion-free Abelian Groups and Rings*, Lecture Notes in Mathematics 931, Springer, New York, 1982.

[Arnold 00] **Arnold, D.M.**, *Abelian Groups and Representations of Finite Partially Ordered Sets*, CMS Books in Mathematics, Springer, New York, 2000.

[Fuchs 70] **Fuchs, L.**, *Infinite Abelian Groups*, Vol. I, Academic Press, New York, 1970.

[Fuchs 73] **Fuchs, L.**, *Infinite Abelian Groups*, Vol. II, Academic Press, New York, 1973.

[Gallian 98] **Gallian, J.A.**, *Contemporary Abstract Algebra*, Fourth Edition, Houghton Mifflin, Boston, 1998.

[Griffith 70] **Griffith, P.A.**, *Infinite Abelian Group Theory*, University of Chicago Press, Chicago, 1970.

[Grimaldi 99] **Grimaldi, R.**, *Discrete and Combinatorial Mathematics*, Fourth edition, Addisom Wesley Longman, Reading, Mass., 1999.

[Kaplansky 69] **Kaplansky, I.**, *Infinite Abelian Groups*, University of Michigan Press, Ann Arbor, 1969.

[Mader 00] **Mader, A.**, *Almost Completely Decomposable Groups*, Gordon and Breach, Amsterdam, 2000.

[Mines, Richman, Ruitenburg 88] **Mines, R., Richman, F. and Ruitenburg, W.**, *A Course in Constructive Algebra*, Universitext, Springer, New York, 1988.

[Moreira 99] **Moreira, C.G.**, *Divisibilidad, Congruencias y Aritmética Módulo n*, Cubo Matemática Educacional, 1, 76-86, 1999.

[Ore 48] **Ore, O.**, *Number Theory and its History*, McGraw-Hill, New York, 1948.