RESEARCH REVIEW JOURNALS
Volume-04
Issue-02
February -2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Theoretical approach of a finite abelian groups

Rupen Chatterjee

Department of Mathematics, Nabagram Hiralal Paul College, Nabagram, Hooghly ,West Bengal Pin:712246 India (Affiliated by Calcutta University)

ARTICLE DETAILS

Article History
Published Online: 20 February 2019

Keywords
Finite, linear algebra, isomorphic

ABSTRACT

It is hopeless to classify all infinite abelian groups, but a good criterion that leads to an interesting classification is that of finite abelian groups. A finite Abelian group G is a p-group with p ∈ N a prime then every element of G has order a power of p. the order of a finite p-group must be a power of p .A finite abelian group is a group satisfying the following equivalent conditions. It is isomorphic to a direct product of finitely many finite cyclic groups. It is isomorphic to a direct product of abelian groups of prime power order and it is also isomorphic to a direct product of cyclic groups of prime power order. An abelian group, also called a commutative group, is a group in which the result of applying the group operation to two group elements does not depend on their order (the axiom of commutativity). They are named after Niels Henrik Abel. An arbitrary finite abelian group is isomorphic to a direct sum of finite cyclic groups of prime power order, and these orders are uniquely determined, forming a complete system of invariants. The automorphism group of a finite abelian group can be described directly in terms of these invariants. The theory had been first developed in the 1879 paper of Georg Frobenius and Ludwig Stickelberger and later was both simplified and generalized to finitely generated modules over a principal ideal domain, forming an important chapter of linear algebra.

1. Introduction

Abelian groups

we will restrict our attention to abelian groups, in other words groups in which the binary operation is commutative. Our aim will be to understand the structure of a large class of abelian groups, including all finite abelian groups. When studying abelian groups, we will adopt the convention (which is quite standard) of using additive notation. This means that the binary operations in our abelian groups will be denoted +, the identity element will be denoted 0 (or 0_A if we wish to emphasise the specific abelian group A), and the inverse of an element x will be denoted by (−x). Since we will always be using the same symbol + for our binary operations, we will usually just refer to the abelian group A rather than the abelian group (A, +). Thus, for example, in Z, Q, R, C it is understood that the binary operation is the usual addition of numbers; in R^n or C^n it is the usual vector addition. A first observation is that, without some sort of restriction, there are too many abelian groups to have any hope of classifying them up to isomorphism. A simple analogy is the classification of (real) vector spaces. A theorem states that every vector space has a basis, and another theorem states that two vector spaces are isomorphic (as vector spaces) if and only if there is a bijection from a basis of one to a basis of the other. Thus the classification of vector spaces up to isomorphism reduces to the classification of sets up to bijection, which sounds easy but in fact depends on the axiomatic foundations of set theory.

Finite abelian groups

Cyclic groups of integers modulo (n, Z/nZ) were among the first examples of groups. It turns out that an arbitrary finite abelian group is isomorphic to a direct sum of finite cyclic groups of prime power order, and these orders are uniquely determined, forming a complete system of invariants. The automorphism group of a finite abelian group can be described directly in terms of these invariants. The theory had been first developed in the 1879 paper of Georg Frobenius and Ludwig Stickelberger and later was both simplified and generalized to finitely generated modules over a principal ideal domain, forming an important chapter of linear algebra. Any group of prime order is isomorphic to a cyclic group and therefore abelian. Any group whose order is a square of a prime number is also abelian. In fact, for every prime number p there are (up to isomorphism) exactly two groups of order p^2, namely Z_{p2} and $Z_p \times Z_p \times Z_p$ .A finite Abelian group is a group for which the elements commute (i.e., AB=BA)for all elements Aand B). Abelian groups therefore correspond to groups with symmetric multiplication tables. All cyclic groups are Abelian, but an Abelian group is not necessarily cyclic. All subgroups of an Abelian group are normal. In an Abelian group, each element is in a conjugacy class by itself, and the character table involves powers of a single element known as a group generator. In the Wolfram Language, the function of finite abelian Group {n_1, n_2, ... }represents the direct product of the cyclic groups of degrees, n_1, n_2, ... No general formula is known for giving the number of nonisomorphic finite groups of a given group order. However, the number of nonisomorphic Abelian finite groups a(n)of any given group order n is given by writing n as

$$n = \prod_i p_i^{\alpha_i},$$

where the p_i are distinct prime factors, then

$$a(n) = \prod_i P(\alpha_i),$$

where p(k)is the partition function, which is implemented in the Wolfram Language as Finite Abelian Group Count[n]. The values of a(n)for n=1, 2, ... are 1, 1, 1, 2, 1, 1, 1, 3, 2, ... (OEIS A000688).

The smallest orders for which, n=1,2, 3, ... nonisomorphic finite abelian Groups exist are 1, 4, 8, 36, 16, 72, 32, 900, 216, 144, 64, 1800, 0, 288, 128, ... (OEIS A046056), where 0 denotes an impossible number (i.e., not a product of partition numbers) of nonisomorphic finite groups. The "missing" values are 13, 17, 19, 23, 26, 29, 31, 34, 37, 38, 39, 41, 43, 46, ... (OEIS A046064). The incrementally largest numbers of Abelian groups as a function of order are 1, 2, 3, 5, 7, 11, 15, 22, 30, 42, 56, 77, 101, ... (OEIS A046054), which occur for orders 1, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, ... (OEIS A046055).

The Kronecker decomposition theorem states that every finite Abelian group can be written as a group direct product of cyclic groups of prime power group order. If the group order of a finite group is a prime p, then there exists a single finite abelian Groups of order p(denoted Z_p) and no non-Abelian groups. If the group order is a prime squared p^2, then there are two Abelian groups (denoted Z_{p2} and $Z_p \times Z_p$.). If the group order is a prime cubed p^3, then there are three Abelian groups (denoted $Z_p \times Z_p \times Z_p$, $Z_p \times Z_{p2}$, and Z_{p3}), and five groups total. If the order is a product of two primes p and q, then there exists exactly one finite abelian Group of order pq(denoted $Z_p \times Z_q$). Another interesting result is that if a(n)denotes the number of nonisomorphic finite abelian Groups of group order n, then

$$\sum_{n=1}^{\infty} a(n)\, n^{-s} = \zeta(s)\,\zeta(2s)\,\zeta(3s)\cdots,$$

where ζ is the Riemann zeta function.

The numbers of Abelian groups of orders $\leq n$are given by 1, 2, 3, 5, 6, 7, 8, 11, 13, 14, 15, 17, 18, 19, 20, 25, ... (OEIS A063966) for n=1, 2, ... Srinivasan (1973) has also shown that

$$\sum_{n=1}^{N} a(n) = A_1 N + A_2 N^{1/2} + A_3 N^{1/3} + O\left[N^{105/407} (\ln N)^2\right],$$

where

$$\prod_{\substack{j=1 \\ j\neq k}}^{\infty} \zeta\left(\frac{j}{k}\right)$$

$$\begin{cases} 2.294856591\ldots & \text{for } k=1 \\ -14.6475663\ldots & \text{for } k=2 \\ 118.6924619\ldots & \text{for } k=3, \end{cases}$$

(OEIS A021002, A084892, and A084893) and the Riemann zeta function. Note that Richert (1952) incorrectly gave A_3 =114. The sums A_K can also be written in the explicit forms

- $\prod_{j=2}^{\infty} \zeta(j)$
- $\zeta\left(\frac{1}{2}\right) \prod_{j=3}^{\infty} \zeta\left(\frac{1}{2} j\right)$
- $\zeta\left(\frac{1}{3}\right) \zeta\left(\frac{2}{3}\right) \prod_{j=4}^{\infty} \zeta\left(\frac{1}{3} j\right).$

De Koninck and Ivic (1980) showed that

$$\sum_{n=1}^{N} \frac{1}{a(n)} = B N + O\left[\sqrt{N}\ (\ln N)^{-1/2}\right],$$

where

$$\prod_p \left\{1 - \sum_{k=2}^{\infty} \left[\frac{1}{P(k-1)} - \frac{1}{P(k)}\right] \frac{1}{p^k}\right\}$$

$$0.752\ldots$$

(OEIS A084911) is a product over primes p and p(n)is again the partition function.

2. Methods and Classification of Finite Abelian Groups

The fundamental theorem of finite abelian groups expresses any such group as a product of cyclic groups:

Suppose G is a finite abelian group. Then G is (in a unique way) a direct product of cyclic groups of order p^k with p prime. Our first step will be a special case of Cauchy's Theorem, which we will prove later for arbitrary groups:whenever p/|G|then G has an element of order p.

Theorem

If G is a finite group, and p/|G| is a prime, then G has an element of order p (or, equivalently, a subgroup of order p).

Proof when G is abelian. First note that if |G| is prime, then G ≃ Z_p and we are done. In general, we work by induction. If G has no nontrivial proper subgroups, it must be a prime cyclic group, the case we've already handled. So we can suppose there is a nontrivial subgroup H smaller than G. Either p/|H|or p/|G/H| . In the first case, by induction, H has an element of order p which is also order p in G so we're done. In the second case, if

g + H has order p in G/H then | g + H|, | g | , so ⟨g⟩ ≃ Z_{kp} for some k, and then kg ∈ G hasorder p. Note that we write our abelian groups additively.

Definition

Given a prime p, a p-group is a group in which every element has order p^k for some k.

A finite group is a p-group if and only if its order is a power of p.

Proof. If G = p^n then by Lagrange's theorem, for any g ∈ G, its order divides p^n, and thus is a (smaller) power of p. Conversely, if |G| is not a power of p, then it has some other prime divisor q, so by Cauchy's theorem, G has an element of order q and thus is not a p-group.

We know that in a cyclic group, any subgroup is determined uniquely by its order. Our first lemma proves a partial converse for p-groups.

Lemma

If G is a finite abelian p-group and G has a unique subgroup H of order p, then is cyclic.

Proof. Again we proceed by induction on |G|, noting that the case |G| = p is obvious. Define φ : G → G by φ(g) = pg, and let K = ker(φ), which consists exactly of those elements of order p (or 1). We find that H ≤ K, so K is nontrivial. But for any nontrivial g ∈ K, the cyclic group (g) has order p, and thus must be H. Thus we see K = H. If K = G, then G≃ Z_p is cyclic and we are done. Otherwise, φ(G) is a nontrivial proper subgroup of G, isomorphic to G/K. By Cauchy's theorem, φ(G) has a subgroup of order p. Since any such subgroup is also a subgroup of G, there is a unique one (namely H = K). Thus we can apply the inductive hypothesis to the group φ(G) ≃ G/K, and we conclude that this group is cyclic. If we write G/K as g + K for some g = e, we claim that g generates G. To check this, it suffices to prove that K ≤ ⟨g⟩ . But by Cauchy, ⟨g⟩ ≤ G has a subgroup of order p, which by uniqueness must be K Combining this lemma with Cauchy's theorem, we see that a noncyclic finite abelian p-group has more than one subgroup of order p, which is the key to the next lemma.

Lemma

If G is a finite abelian p-group and C is a cyclic subgroup of maximal order, then G = C⊕H for some subgroup H.

Proof. Again, we proceed by induction on |G|, noting that when G is cyclic, C = G and H = {e}. When G is not cyclic, we have just shown it has more than one subgroup of order p, while the cyclic group C has a unique such subgroup. So let K ≤ G be a subgroup of order p not contained in C. Because K has prime order, K ∩ C = {e}, which implies

(C + K)/K≃ C.

Given any g ∈ G, the order of g + K in G/K divides |g|, which is at most |C|. Thus the cyclic subgroup (C + K)/K≃ C has maximal order in G/K, and we can apply the inductive hypothesis to prove that G/K = (C + K)/K⊕ H' for some H' ≤ G/K. The preimage of H' under the map G → G/K is a group H with K ≤ H ≤ G. But G/K = (C + K)/K⊕ H/K means that G = (C + K) + H = C + (K + H) = C + H. Since H ∩ (C + K) = K, we have

H ∩ C = {e}, so by definition G = C⊕H.

Theorem

Any finite abelian group is a direct s um of cyclic subgroups of prime-power order.

Proof. For any prime p dividing |G|, we set G_p := { g : |g| = p^k} and $G_{p'}$:= { g : p ≠|g|}. Then by Cauchy's theorem, G_p is nontrivial and is a p-group. Now if g ∈ G has order p^km (with p|m), then p^kg ∈ $G_{p'}$ and mg ∈ G_p. Since p^k and m are relatively prime, there are r and s with rp^k + sm = 1, so we can write g = r(p^kg) + s(mg) as a sum of elements in $G_{p'}$ and G_p. This shows that G = G_p ⊕ G_p .

Repeating this process for the remaining primes dividing the order of $G_{p'}$ we can decompose G as a direct sum of p-groups for different p. So it suffices to prove the theorem for p-groups like G_p, which have order p^k. We do this by induction on k.Let C be a cyclic subgroup of G_p of maximal order.By the last lemma,G=C⊕H with H <| G| . By the inductive hypothesis, H is a direct sum of cyclic subgroups, and we are done.

We note that the decomposition of G given in the theore m is unique. Certainly, the subgroup G_p is uniquely defined for any p. Now suppose a p-group G_p has been expressed as a product of cyclic groups in two ways: as H_1× ..... ×H_m and as K_1× ..... ×K_n, with |H_i | ≥ |H_j | and |K_i | ≥ | K_j | when i < j. Then |H_1| = |K_1 | since each of these must equal the maximal order of an element of G_p. Proceeding by induction, we find that the two decompositions are really the same. However, we should note, for instance, that although G = Z_p× Z_p has no other expression as a product of cyclic groups,

there are many pairs of subgroups H and K of order p for which G = H ⊕K. In this example, for any nonzero elements a and b, we have G = ⟨a⟩ ⊕ ⟨b⟩ unless a is a multiple of b.

We are now reduced to the study of finite abelian p- groups. There are many examples of these - such as Z*p*, Z*p*2 , Z*p* × Z*p*, etc. Indeed, for any finite sequence σ = (t1,...,tk) of positive integers, there is a finite abelian group Aσ = Z*p*t1 ×⋯× Z*p*tk . These are all different.

Well, since A × B ≃ B × A (exercise), they can only be different up to reordering the factors, so we may assume (for example) that the sequence of positive integers (t1,...,tk) is non-decreasing: t1 ≤⋯≤ tk. The groups Aσ for different σ are then non-isomorphic. To see this, one can easily check that the largest order of any element of Aσ is ptk where tk is the largest term of the sequence σ, and then argue by induction on the length k of the sequence. Finally, we show that the groups Aσ just defined are the only finite abelian *p*-groups, up to isomorphism. Let A = Zn/K be a finite abelian *p*- group, where n is chosen to be as small as possible, and K is a rank n subgroup of Zn.

3. Fundamental Concepts of Finite Abelian Groups

Finitely generated abelian group

In abstract algebra, an abelian group (G, +) is called finitely generated if there exist finitely many elements x_1, ..., x_n in G such that every x in G can be written in the form $x = n_1x_1 + n_2x_2 + ... + n_nx_n$ with integers n_1, ..., n_n. In this case, we say that the set { x_1 x_2..... x_n } is a generating set of G or that x_1 x_2..... x_n generate G. Every finite abelian group is finitely generated. The finitely generated abelian groups can be completely classified.

Example

- The integers,(Z,+), are a finitely generated abelian group.
- The integers modulo ,n , (Z/nZ,+) are a finite (hence finitely generated) abelian group.
- Any direct sum of finitely many finitely generated abelian groups is again a finitely generated abelian group.
- Every lattice forms a finitely generated free abelian group.

There are no other examples (up to isomorphism). In particular, the group (Q,+)of rational numbers is not finitely generated: if x_1 x_2..... x_n are rational numbers, pick a natural number k coprime to all the denominators; then 1/k cannot be generated by if x_1 x_2..... x_n. The group (Q*,+) of non-zero rational numbers is also not finitely generated. The groups ofreal numbers under addition(R,+) and non-zero real numbers under multiplication (R*,+) are also not finitely generated. The fundamental theorem of finitely generated abelian groups can be stated two ways, generalizing the two forms of the fundamental theorem of finite abelian groups. The theorem, in both forms, in turn generalizes to the structure theorem for finitely generated modules over a principal ideal domain, which in turn admits further generalizations.

Isomorphism

In mathematics, an isomorphism is a mapping between two structures of the same type that can be reversed by an inverse mapping. Two mathematical structures are isomorphic if an isomorphism exists between them.

The interest in isomorphisms lies in the fact that two isomorphic objects have the same properties (excluding further information such as additional structure or names of objects). Thus isomorphic structures cannot be distinguished from the point of view of structure only, and may be identified. In mathematical jargon, one says that two objects are the same up to an isomorphism.

An automorphism is an isomorphism from a structure to itself. An isomorphism between two structures is a canonical isomorphism if there is only one isomorphism between the two structures (as it is the case for solutions of a universal property), or if the isomorphism is much more natural (in some sense) than other isomorphisms. For example, for every prime number *p*, all fields with *p* elements are canonically isomorphic, with a unique isomorphism. The isomorphism theorems provide canonical isomorphisms that are not unique.

The term isomorphism is mainly used for algebraic structures. In this case, mappings are called homomorphisms, and a homomorphism is an isomorphism if and only if it is bijective.

In various areas of mathematics, isomorphisms have received specialized names, depending on the type of structure under consideration. For example:

- An isometry is an isomorphism of metric spaces.
- A homeomorphism is an isomorphism of topological spaces.
- A diffeomorphism is an isomorphism of spaces equipped with a differential structure, typically differentiable manifolds.
- A permutation is an automorphism of a set.

Category theory, which can be viewed as a formalization of the concept of mapping between structures, provides a language that may be used to unify the approach to these different aspects of the basic idea.

Cyclic Groups

Let us say that a group is cyclic if it is a cyclic subgroup of itself. We have seen that any cyclic subgroup is isomorphic either to Z or to Zn for some n. On the other hand, Z = ⟨1⟩is cyclic, and Zn = ⟨1⟩is cyclic for each n. Hence the cyclic groups are classified up to isomorphism by their order. Cyclic groups are abelian, but of course not every abelian group is cyclic. Example. The Klein 4-group K = $Z_2 \times Z_2$ of order 4 is abelian. It cannot be cyclic because it does not contain an element of order 4.

Here are some elementary properties of cyclic groups .

Every subgroup of a cyclic group is cyclic. Every quotient group of a cyclic group is cyclic.

Let H be a subgroup of Z. If H = {0} then H = ⟨0⟩ is cyclic. If H ≠{0} then H contains at least one positive integer. Let n be the least positive integer contained in H. Then ⟨n⟩ = nZ ⊂ H. If H ≠nZ, then there is an integer k ∈ H with k ∈/ nZ. Dividing k by n, we find k = nq + r with q, r ∈ Z and 0 <r <n, But then r = k − nq ∈ H, contradicting the choice of n. Hence H = nZ ⟨n⟩ is cyclic. Now let H be a subgroup of Zn for some n, and let f : Z → Z/nZ ≃ Zn be the quotient homomorphism (f(k) = k mod n). Then Ĥ := {k ∈ Z, f(k) ∈ H} is a subgroup of Z, so cyclic. Say Ĥ = ⟨m⟩ = mZ. Then H = f (Ĥ) = mZn = ⟨m⟩ is a cyclic subgroup of Zn.

If Q is a quotient group of Z, then Q = Z/K where K is a subgroup of Z. Either K = {0}, in which case Z/K ≃ Z is infinite cyclic, or K = nZ for some n > 0, in which case Z/K ≃ Zn is cyclic of order n. Finally, if Q is a quotient group of Zn, then there are surjective homomorphisms Z → Zn → Q. The composite of these homomorphisms is also surjective, so Q is also a quotient group of Z. We have just shown that such groups are cyclic. Any group whose order is a prime number is cyclic.

Suppose that (G, ∗) is a group whose order is a prime number *p*. (Note that we cannot a priori assume that the group is abelian, since it is not part of the hypothesis.) Since |G| = *p* > 1, there is at least one element a ∈ G which is not the identity element, and hence has order greater than 1. By Lagrange's Theorem, the order of a divides the prime number p, and hence it must be equal to *p*. Thus the cyclic subgroup hai has order *p* = |G|, so G = ⟨a⟩ is a cyclic group.

Here is a slightly less elementary property. Two positive integers m, n are said to be coprime if they have no common prime factors. For example, 24 and 35 are coprime, while 77 and 224 are not coprime (both being divisible by 7).

The Chinese Remainder Theorem

Let $n_1, n_2,..., n_k$ be positive integers which are pairwise coprime that is, n_i and n_j are coprime whenever $1 \le i$

Let $N = n_1 n_2... n_k$ be their product. Then

$Z_N \simeq Zn_1 \times Zn_2 \times \cdots \times Zn_k$

Proof. It suffices to prove this result in the case where k = 2. The general case follows by induction on k: assume inductively that $Zn_2 \times \cdots \times Zn_k \simeq Z_{N'}$, where $N' = n_2... n_k = N/ n_1$. Note that n_1 and N' are coprime, so by the case k = 2 we have $Zn_1 \times Z_{N'} \simeq Z_N$ Hence we may assume that m, n are coprime positive integers, and we are required to prove that $Z_m \times Z_n \simeq Z_{mn}$

Recall that $Z_m \simeq Z/mZ$, and similarly $Z_n \simeq Z/nZ$. Define a homomorphism f : Z → (Z/mZ) × (Z/nZ) by f(t)=(t + mZ, t + nZ). Then Ker(f) = {t ∈ Z; t ∈ mZ & t ∈ nZ} = mZ ∩ nZ = mnZ. (Since m, n are coprime, an integer t is divisible by m and by n if and only if it is divisible by mn.) By the First Isomorphism Theorem, Im(f) ≃ Z/Ker(f) = Z/mnZ, which has order mn. But (Z/mZ) × (Z/nZ) also has order mn. Hence Im(f) is the whole of (Z/mZ) × (Z/nZ). Thus

$Z_{mn} \simeq Z/mnZ \simeq (Z/mZ) \times (Z/nZ) \simeq Z_m \times Z_n$.

Direct product

Let A and B be two arbitrary groups, not necessarily with the same binary operations. We de ne the direct product of A and B to be

$A \times B = \{(a, b) \mid a \in A, b \in B\}$

This two-dimensional set is again a group if we consider the operation where for every two elements (a, b), (c, d) ∈ A × B, we set (a, b)(c, d) = (ac, bd).

In some texts, our de nition of direct product may be introduced by the name external direct product. You will soon see why the adjective is added, but rst let us observe some elementary facts which are not hard to verify and which are intuitively clear anyhow.

Proposition

1. The following properties hold which concern the direct product of groups.

The commutative property: A × B ≃ B × A. Think of swapping places between the components; doing so does not a ect the structure of the group .The associative property:

A × (B × C) ≃ (A × B) × C. This allows us to simply write multiple products without brackets, e.g., A × B × C.

2.The substitution property: If $A \simeq A'$ and $B \simeq B'$, then $A \times B \simeq A' \times B'$.

3.The identi cation property: We may treat the group A as a subgroup of A×B by identifying A with the subgroup A × {e}, where e denotes the identity element. Of course, by symmetry, we may also call the coordinate B a subgroup of A × B, i.e., {e} × B.

Another result which we have not discussed in class is the useful criterion for ex-pressing an arbitrary group as a direct product of its subgroups.

Theorem Let G be a group with two normal subgroups H and K, with the condi-tions that H ∩ K = {e} and HK = G. Then G ≃ H × K.

We remark frst that we will be concerned with only abelian groups, where all subgroups are automatically normal.

The hypothesis of Theorem is sometimes used as the de nition of G being the internal direct product of H and K. In other words, Theorem 2 states that internal implies external. Conversely, given G = H × K, we have two normal subgroups, i.e., H × {e} ≃

H and {e} × K ≃ K, whose internal direct product recovers G. Hence, the two notions of external and internal direct products are actually equivalent.

Proof. We frst show that every element of H commutes with any other of K. Let h∈ H and k ∈ K. We note that $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$ because K is normal, and similarly $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$. However, H ∩ K = {e}, so we see that $hkh^{-1}k^{-1} = e$, i.e., that hk = kh. This result opens the way for a homomorphism θ : H × K → HK depaned by θ(h, k) = hk. As we can check,

$$\theta((h, k)(h', k')) = \theta(hh', kk') = hh'kk' = hkh'k' = \theta(h, k)\theta(h', k')$$

Since HK = G, we are only left with showing that θ is one-to-one and onto. Well, onto is quite obvious by the very de nition of HK. For one-to-one, let θ(h, k) = θ(h′, k′), so that hk = h′k′. Then $h^{-1}h' = k(k')^{-1}$. The left side belongs to H and the right to K. This is possible only if both be the identity element. Thus h = h′ and k = k′,

completing the proof.

To make the result complete, we need to extend Theorem inductively to three or more subgroups.

Let G be a group with three normal subgroups H, K, and L, such that H ∩ K = {e}, HK ∩ L = {e}, and HKL = G. Prove that G ≃ H × K × L.

The fundamental theorem

The fundamental theorem essentially states that every finite abelian group is isomorphic to a direct product of cyclic groups. Recall that every cyclic group of order n is given by the modular integers Z_n under addition mod n. Hence, to illustrate, an abelian group of order 1200 may actually be isomorphic to, say, the group $Z_{40} \times Z_6 \times Z_5$. Furthermore, let us recall the Chinese remainder theorem, which we shall abbreviate CRT, and which says that if gcd(m, n) = 1, then $Z_{mn} \simeq Z_m \times Z_n$. In the preceding example, we may then replace Z_{40} by $Z_23 \times Z_5$, and Z_6 by $Z_2 \times Z_3$. Therefore, we will state the fundamental theorem like this: every nite abelian group is the product of cyclic groups of prime power orders. The collection of these cyclic groups will be determined uniquely by the group G. Here is why.

Suppose we have two direct products of order 1200, e.g.,

$$A=Z_23\times Z_5\times Z_2\times Z_3\times Z_5$$

$$B=Z_52\times Z_22\times Z_22\times Z_3$$

It is easy to see why A≃ B: the group A has an element of order 8, i.e., (1, 0, 0, 0, 0). On the other hand if (a, b, c, d) ∈ B, then $(a, b, c, d)^m = (0, 0, 0, 0)$ where m is the least common multiple of 25, 4, and 3. Since m is not a multiple of 8, we conclude that there is no elements of order 8 in B.

In general, to show that such isomorphism is impossible, simply take any prime factor p for which there is a discrepancy between left and right. Say, Z_pj and Z_pk be the maximal components of A and B, respectively, with j > k. (If j = k, the cancellation property allows us to omit the factor Z_pk and start over with the rest.) Then A would have an element of order p^j , whereas B would not, so the two can't possibly be the same groups.

Hence, we will now formally state the fundamental theorem of nite abelian groups, abbreviated FTFAG, as follows.

Theorem

Every nite abelian group is isomorphic to the direct product of a unique collection of cyclic groups, each having a prime power order.To remark, by the word collection used in the theorem, we mean a multiset, i.e., where repetition of elements is allowed but ordering them is not important.

Elements of the proof

The uniqueness part in statement of FTFAG is already explained. To make the proof more readable, we go by step-by-step observations. As a matter of fact, the rst one is an easy exercise for you to warm up before the long journey.

Let G be a group with identity element e and a normal subgroup H, and let x ∈ G. Suppose that the element Hx has order n in the factor group G/H. Then x has order in G a multiple of n.The truth is, the preceding exercise is needed to establish the next result, which is actually the famous Cauchy's theorem applied to abelian groups. We talk about Cauchy's theorem in the lecture but did not get to really prove it, so we have no choice but to buy the theorem right here.

Theorem

Let p be a prime number. If any abelian group G has order a multiple of *p*, then G must contain an element of order *p*.Proof. Let |G| = k*p* for some k ≥ 1. In fact, the claim is true if k = 1 because any group of prime order is a cyclic group, and in this case any non-identity element will have order p. We proceed by induction. Take any non-identity element x ∈ G, say of order m. We are done

if p divides m, for then $x^{m=p}$ will have order *p*. Otherwise, consider the factor group $G' = G/\ x$, of order $|G'| = kp/m$. Since m is not a multiple of *p*, we may write $|G'| = jp$ for some $j < k$. We apply the induction hypothesis to conclude that G' contains an element of order p. According to the preceding exercise,

then G contains an element of order a multiple of p, and that succes.

Lemma

Let G be an abelian group with identity e. For a xed positive integer n, the set $H = \{x \in G \mid x^n = e\}$ is a subgroup of G.

Proof. If $a \in H$ then $a^{-1} \in H$ since $(a^{-1})^n = (a^n)^{-1} = e$ moreover if $a,b \in H$ then being abelian $(ab)^n = a^n b^n = e$ and $ab \in H$. Thus H passes the subgroup test. Now in order to conveniently refer to this subgroup H stated in the lemma, we shall give it a special notation. De nition. Let G be an abelian group with identity e and let n be a xed positive integer. We de ne the subgroup G(n) of G by $G(n) = \{x \in G \mid x^n = e\}$.

Lemma

Suppose that gcd(m, n) = 1, and let G be an abelian group of order mn. Then $G \simeq G(m) \times G(n)$.

Proof. To establish this lemma, we will employ Theorem, showing that $G(m)G(n) = G$ and $G(m) \cap G(n) = \{e\}$. The second part is easy: if $x \in G(m)$ then the order of x in G must divide m, and similarly with n in place of m. With gcd(m, n) = 1, we see that $G(m) \cap G(n)$ contains only elements of order one, i.e., only the identity element.

Next, note that for every $x \in G$, we have $x^m \in G(n)$ because $(x^m)^n = x^{|G|} = e$. And similarly, $x^n \in G(m)$. Now gcd(m, n) = 1 also implies that we can nd a, $b \in Z$ such that 1 = am + bn. Then for every $x \in G$, we have

$$x = x^{am+bn} = (x^m)^a (x^n)^b \in G(n)G(m)$$

This establishes the claim that G(m)G(n) = G.

Lemma

Suppose that gcd(m, n) = 1, and let G be an abelian group of order mn. Then $|G(m)| = m$ and $|G(n)| = n$.

Proof. We already have $G \simeq G(m) \times G(n)$. The case m = 1 would be trivial, for then G(m) = {e}. So we assume there is a prime p which divides m. We claim that |G(n)| is not a multiple of p, for otherwise by Cauchy's theorem, G(n) would contain an element of order p. It would follow by the de nition of G(n) that p would divide n, which is impossible as m and n have no common factors. By symmetry, we also conclude that if a prime q divides G(n), then q does not divide G(m). However, we know that $|G(m)| \times |G(n)| = mn$. Hence by factoring mn into prime numbers,

It is necessary to have |G(m)| = m and |G(n)| = n.

The preceding two lemmas can be easily extended to three or more subgroups. If n is expressed as the product of distinct prime powers,

$$n = p^{e_1}{}_1 \times p^{e_2}{}_2 \times \cdots \times p^{e_k}{}_k$$

and if G is an abelian group of order n, then

$$G \simeq G(p^{e_1}{}_1) \times G(p^{e_2}{}_2) \times \cdots \times G(p^{e_k}{}_k)$$

where each $|G(p^{e_i}{}_i)| = p^{e_i}{}_i$. Thus, we will now establish FTFAG by showing just one more fact: that every abelian group of a prime power order is a direct product of cyclic groups, each having a prime power order.

Lemma

Let *p* be a prime number and let G be an abelian group of order p^k, for any integer $k \geq 1$. Then G is isomorphic to the direct product of cyclic groups.

Note that the cyclic groups satisfying the statement of the lemma will, of necessity, each have order a power of *p*.

Proof. We use induction on k. The case k = 1 gives a cyclic group G of order *p*, so there is nothing to prove. Otherwise, since there is only one prime involved, we may consider element $g \in G$ of order p^m, such that $x^{pm} = e$ for all $x \in G$. Moreover, let H be a subgroup of G which is maximal with respect to the condition $g \cap H = \{e\}$. We will show that g H = G, so that $G \simeq g \times H$. Then the proof will complete by applying the induction hypothesis on H since H itself is an abelian group of order a power of p, but less than that of G.By contradiction, suppose there exists $c \in G$, but c/g H. We may assume that $c^p \in g$ H, for if not, simply replace c by c^p. And if still c^{p2}/g H, replace c^{p2} by c^{p3} , etc. This process will not take more than m steps. We may write $c^p = g^r h$, for some $h \in H$. Since $(c^p)^{pm\ 1} = e$, we have $g^{rpm\ 1} \in H$, and so $g^{rpm\ 1} = e$ by the condition $g \cap H = \{e\}$. In particular, g^r does not generate g . It follows that $\gcd(r, p^m) > 1$, i.e., that p divides r. Now let $s = -r/p$, and consider the subgroup K of G given by $K = cg^s$ H. We note that cg^s/H because c/g H. Thus, H is a proper subgroup of K. We will nish the proof by showing that $g \cap K = \{e\}$, which contradicts the maximal choice of the subgroup H. Every element $y \in K$ is of the form $y = (cg^s)^t h_2$ for some $h_2 \in H$. Since

$$(cg^s)^p = c^p(g^{-r/p})^p = c^p g^{-r} = h \in H$$

we note that if t is a multiple of p, then $y \in H$. In that case, we have that $y \neq g$ unless $y = e$. On the other hand, suppose now $\gcd(t, p) = 1$. Then there exist $u, v \in Z$ such that $tu = 1 + pv$. (Think of elements of the multiplicative group U_p.) It follows that

$y^u = (cg^s)^{tu} h_2^u = (cg^s)^{1+pv} h_2^u = (cg^s)(cg^s)^{pv} h_2^u = (cg^s)h^v h_2^u$

So if $y \in g$, then $c \in g H$, which is false. We have therefore shown that the onlyelement in $\langle g \rangle \cap K$ is the identity.

4. Application and Results

The fundamental theorem readily gives us a means to the classification of all nite abelian groups according to their orders. We illustrate rst with three examples.

1.The group $U_{12} = \{1, 5, 7, 11\}$ under multiplication mod 12 is not cyclic. By FTFAG, there are only two abelian groups of order 4, i.e., Z_4 and $Z_2 \times Z_2$. We conclude that $U_{12} \simeq Z_2 \times Z_2$.

2.The group U_{60} has $\phi(60) = 16$ elements. There are ve abelian groups of order 16, i.e.,

$G_1 = Z_24$
$G_2 = Z_23 \times Z_2$
$G_3 = Z_22 \times Z_22$
$G_4 = Z_22 \times Z_2 \times Z_2$

$$G_5 = Z_2 \times Z_2 \times Z_2 \times Z_2$$

Meanwhile, we look at the order $|x|$ for each element $x \in U_{60}$, i.e.,

x	1	7	11	13	17	19	23	29	31	37	41	43	47	49	53	59
|x|	1	4	2	4	4	2	4	2	2	4	2	4	4	2	4	2

Since we have elements of order 4, but not 8, we rule out G_1, G_2, and G_5. Whereas for G_3, only three elements have order 2, i.e., (0, 2), (2, 0), and (2, 2). Therefore, we go with G_4|thus $U_{60} \simeq Z_4 \times Z_2 \times Z_2$.Consider the group U_{63} of order $\phi(63) = 36$, again not cyclic. There are four abelian groups of this order:

$G_1 = Z_22 \times Z_32 \simeq Z_{36}$

$G_2 = Z_22 \times Z_3 \times Z_3$
$G_3 = Z_2 \times Z_2 \times Z_32$

$G_4 = Z_2 \times Z_2 \times Z_3 \times Z_3$

And again, we look at the table of orders in U_{63} and nd only elements of orders 1, 2, 3,and 6. There is no doubt,

$U_{63} \simeq Z_2 \times Z_2 \times Z_3 \times Z_3 (\simeq Z_6 \times Z_6)$.

(Here is another way to study the orders in U_{63} in a glance. The group U_7 has order 6, hence $x^6 \equiv 1 \pmod 7$ for all integers x with $\gcd(x, 7) = 1$. Similarly, $x^6 \equiv 1 \pmod 9$ if $\gcd(x, 9) = 1$, because U_9 too has order 6. Since $\gcd(7, 9) = 1$, CRT applies and $x^6 = 1$ for all $x \in U_{63}$. This e xplains why the order of every element in U_{63} must divide 6.) For each given n, identify the group U_n by writing it as the direct product of cyclic groups of prime power orders.

(a) n = 27 (b) n = 32 (c) n = 45 (d) n = 72

An interesting question follows: Given a positive integer n, how do we determine the number of distinct abelian groups of order n.We can see in the three examples above a pattern that plays on the exponent of each prime appearing in the factorization of n. For example, the case $n = 16 = 2^4$ relies completely upon the different ways we partition the exponent 4 into positive integers. This leads us to the following definition.

Where n ranges through the positive integers, de ne the partition function $p(n)$ to stand for the number of di erent partitions of n into positive integers. For instance $p(4) = 5$, having seen we can partition 4, i.e.,

4 = 4

4=3+1

4=2+2

4=2+1+1

4=1+1+1+1

This function enables us to better express the number of distinct abelian groups of a given order, as follows.

Theorem

Let n denote a positive integer which factors into distinct prime powers, written $n = \prod p^{e_k}_k$. Then there are exactly $\prod p(e_k)$ distinct abelian groups of order n.

In particular, when n is square-free, i.e., all $e_k = 1$, then there is a unique abelian group of order n given by $Z_{p1} \times Z_{p2} \times \cdots \times Z_{pk}$, which is just the cyclic group Z_n, if we may borrow CRT again.

Count how many distinct abelian groups of the given order n.

(a) n = 1024 (b) n = 27000 (c) n = 30030 (d) n = 31104

The next observation will lead to an alternate but equivalent form in which FTFAG can be presented. Let's say we work with the group

$G=Z_24\times Z_22\times Z_2\times Z_3\times Z_3\times Z_53\times Z_53\times Z_5\times Z_5\times Z_7$

Let us write out these prime powers in matrix format, one row for each prime base, left-justi ed, ordered from the greatest exponent to the least, as follows.

$$\begin{matrix} 2^4 & 2^2 & 2 \\ 3 & 3 & \\ 5^3 & 5^3 & 5 & 5 \\ 7 & & & \end{matrix}$$

Observe that every column consists of distinct prime powers. As you probably have guessed, we then apply CRT columnwise, to conclude that

$G\simeq Z_{42000} \times Z_{1500} \times Z_{10} \times Z_5$

Now going from left to right, the columns successively lose some primes without ever gaining new ones. Hence, the sequence of the cyclic group orders, e.g., 42000, 1500, 10, 5, consists of successive divisors|each number divides the preceding number. In other words, the direct product is now made up of nested cyclic subgroups, since each factor can be viewed as a subgroup of the preceding one. Thus, we state FTFAG alternately in this second form. Again, you can easily supply the proof for uniqueness.

Theorem

Every finite abelian group is isomorphic to the direct product of a unique collection of cyclic groups of the form $Z_{n1} \times Z_{n2} \times \cdots \times Z_{nk}$, with the condition that each n_i is a multiple of n_{i+1} for $0 < i < k$.

Prove that if a group G is expressible as a direct sum such as described in FTFAG, then the cyclic group factors are uniquely determined by G.

Another useful consequence of FTFAG is a statement concerning the subgroups of an abelian group. The result is somewhat an extension of Cauchy's Theorem 6. We will make this observation our last one for now.

Theorem

Let m be any positive integer and let G be an abelian group of order a multiple of m. Then there exists a subgroup of G which has order m.

We give rst an illustration of this claim which will also serve as a model for writing the proof of Theorem. Suppose that G is a group of order 1,120,210,560, given by

$G=Z_23\times Z_23\times Z_2\times Z_32\times Z_32\times Z_32\times Z_5\times Z_73\times Z_7$

This big number is a multiple of 6048; how do we nd a subgroup of order 6048.First, we look at the factorization of 6048, i.e., $6048 = 2^5 \times 3^3 \times 7$. Then we select the cyclic group factors of G corresponding to these prime factors, i.e., 2, 3, 7, largest exponent rst, just enough to exceed 2^5, 3^3, and 7. If necessary, we will take a subgroup of the cyclic group in order to match the total exponent that we need for each prime.

2^3 2^3 2 3^2 3^2 3^2 5 7^3 7

|3 |3 |2 |2 |3
2 2 3 3 7

|2 | |
2 3 7

In this way, the desired subgroup of order 6048 comes out to be

$Z_2 3 \times Z_2 2 \times Z_3 2 \times Z_3 \times Z_7$

Note that we have freely used the fact that every cyclic group has a (unique) subgroup of order any number that divides the order of the group. A bit more partitions The partition function p(n) is a fruitful topic in advanced number theory. It will not do justice, and rather out of place, if we attempt to write a short chapter on partitions simply because we encounter p(n) in discussing nite abelian groups. Nevertheless, we just want to mention a few results which more or less relate to the evaluation of $p(n)$.We inspect that $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 7$,...up to $p(10) = 42$

The sequence then increases quite rapidly, exceeding one million partitions with mere n = 61. In fact, the growth of $p(n)$ is known to be sub-exponential and, more speci cally, $p(n)$ is asymptotically close to the function

$$\mathbf{P(n)} = \frac{\prod \sqrt{2n/3}}{4n\sqrt{3}}$$

What we mean is that $\lim \mathbf{P(n)}/p(n) = 1$ as $n \to \infty$. For example, $\mathbf{P(10^4)} \approx 36.32 \times 10^{105}$, and that is roughly big $p(10000)$.

In dealing with a rapidly growing sequence like p(n), one would hope to nd a recur-rence relation of some sort. With $p(n)$, there is no explicit way to de ne a recurrence relation, but we may get help from the so-called intermediate partition functions.

Definition. Let $p_k(n)$ denote the number of partitions of n into positive integers, each no smaller than k, where $1 \le k \le n$. In particular, $p_1(n) = p(n)$.

Note that the partitions belonging to $p_{k+1}(n)$ form a subset of those belonging to $p_k(n)$. Moreover, if a partition belongs to $p_k(n)$ but not to $p_{k+1}(n)$, then the partition must be composed of a k term plus another partition belonging to $p_k(n - k)$, and vice versa. We express this relation into the following identity.

$$p_k(n) = p_{k+1}(n) + p_k(n - k)$$

This is our recurrence relation. To start off , note that $p_k(n) = 1$ whenever $n/2 < k \le n$ as it is impossible to partition n into two or more terms each of which is larger than half of n. We then build a table, rows for n and columns for k, and start lling in by rows according to (1), right to left, with the right half all 1's. The leftmost entry is what we are after, i.e., $p_1(n) = p(n)$. For convenience, we omit the terms $p_k(n) = 0$ which apply when $k > n$.

n	$p(n)$	$p_2(n)$	$p_3(n)$	$p_4(n)$	$p_5(n)$	$p_6(n)$	$p_7(n)$	$p_8(n)$	$p_9(n)$	$p_{10}(n)$
1	1									
2	2	1								
3	3	1	1							
4	5	2	1	1						
5	7	2	1	1	1					
6	11	4	2	1	1	1				
7	15	4	2	1	1	1	1			
8	22	7	3	2	1	1	1	1		
9				2	1	1	1	1	1	
10					2	1	1	1	1	1

To make yourself familiar with the recursive pattern, try to complete the remaining two rows, beginning with $p_3(9) = p_4(9) + p_3(9-3)$, and make sure you end with $p(10) = 42$.

Hence, the coe cient of x^n is composed of how many 1's (from the frst bracket), 2's (second bracket), 3's (third), etc., whose sum is n. The number of such combinations is just the number of ways we partition n into positive integers, thus $p(n)$. Generating functions can sometimes be used to derive identities involving restricted partitions.

5. Conclusion

We have proved the following result, which almost classifies finite abelian groups. Any finitely generated abelian group is a direct product of cyclic groups. This is only an 'almost' classification, since the representation of finite abelian groups as direct products of cyclics is not unique. Indeed the Chinese Remainder Theorem explicitly tells us how to further decompose cyclic groups as direct products of cyclic groups. On the other hand, we can obtain a 'canonical' decomposition as follows. Firstly, decompose as a direct product of z_r and a finite abelian group. Secondly, decompose the finite part into its primary components, each of which has a unique expression as a direct product of cyclic groups. Finally, collect together the largest cyclic direct factor for each prime number involved, and express their direct product as a cyclic group using the Chinese Remainder Theorem; repeat with the second-largest factor for each prime, and so on.

Let A be a finitely generated abelian group. Then there is a unique nonnegative integer r and a unique sequence $m_1, m_2,..., m_k$ of positive integers, such that mi divides m_{i+1}

for $1 \le i \le k - 1$ and $A \simeq z_r \times Z_{m1} \times \cdots \times Z_{mk}$.

The direct product decomposition of a finitely generated group A given in this Theorem is called canonical.To find the canonical decomposition of

$A = Z_{36} \times Z_{40} \times Z_{175}$

we first find the p-primary component for each prime p dividing the order of A:

$|A| = 36 \cdot 40 \cdot 175 = (2^2 \cdot 3^2) \cdot (2^3 \cdot 5) \cdot (5^2 \cdot 7)$.

The primes concerned are 2, 3, 5, 7. The p-primary components are

$A_2 = Z_4 \times Z_8 \times Z_2$, $A_3 = Z_9$, $A_5 = Z_5 \times Z_{25}$, $A_7 = Z_7$

For each prime, take the largest of the factors, ie Z_8, Z_9, Z_{25} and Z_7, and combine then using the Chinese Remainder Theorem:

$Z_8 \times Z_9 \times Z_{25} \times Z_7 \simeq Z_{12600}$

For the primes 3, 7 there is only one factor; for 2, 5 the second largest factor is Z_4, Z_5 respectively. Combining these gives

$Z_4 \times Z_5 \simeq Z_{20}$

For the prime 5, that is all; while for the prime 2 there is one more factor Z_2. Thus the canonical decomposition of A is

$A \simeq Z_2 \times Z_{20} \times Z_{12600}$

References

1.Arnold, D. M. and Rangaswamy, K. M. (Eds.). Abelian Groups and Modules. New York: Dekker, 1996.

2.DeKoninck, J.-M. and Ivić, A. Topics in Arithmetical Functions: Asymptotic Formulae for Sums of Reciprocals of Arithmetical Functions and Related Fields. Amsterdam, Netherlands: North-Holland, 1980.

3.Erdős, P. and Szekeres, G. "Über die Anzahl abelscher Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem." Acta Sci. Math. (Szeged) 7, 95-102, 1935.

4.Finch, S. R. "Abelian Group Enumeration Constants." §5.1 in Mathematical Constants. Cambridge, England: Cambridge University Press, pp. 273-278, 2003.

5.Fuchs, L. and Göbel, R. (Eds.). Abelian Groups. New York: Dekker, 1993.

6.Kendall, D. G. and Rankin, R. A. "On the Number of Abelian Groups of a Given Order." Quart. J. Oxford 18, 197-208, 1947.

7.Kolesnik, G. "On the Number of Abelian Groups of a Given Order." J. reine angew. Math. 329, 164-175, 1981.

8.Neumann, P. M. "An Enumeration Theorem for Finite Groups." Quart. J. Math. Ser. 2 20, 395-401, 1969.

9.Pyber, L. "Enumerating Finite Groups of Given Order." Ann. Math. 137, 203-220, 1993.

10.Renteln, P. and Dundes, A. "Foolproof: A Sampling of Mathematical Folk Humor." Notices Amer. Math. Soc. 52, 24-34, 2005.

11.Richert, H.-E. "Über die Anzahl abelscher Gruppen gegebener Ordnung I." Math. Zeitschr. 56, 21-32, 1952.

12.Sloane, N. J. A. Sequences A000688/M0064, A063966, and A084911 in "The On-Line Encyclopedia of Integer Sequences."

13.Srinivasan, B. R. "On the Number of Abelian Groups of a Given Order." Acta Arith. 23, 195-205, 1973.

14.Gabriel Navarro, On the fundamental theorem of finite abelian groups, Amer. Math. Monthly, February 2003

