The Fundamental Theorem of Finite Abelian Groups

Zak Basta
Edgar Estrada

Abstract

The purpose of this paper is understand and admire the complexities that arise when studying finite abelian groups, as well as introduce techniques with which one can simplify the calculations and further explore the encoded data of a structure with such properties as above. As such, it is the aim of the authors to provide intuitive language to convey a concept and then introduce formal definitions.

Introduction

An **abelian** group is a group G in which $ab = ba, \forall a, b \in G$. This property, as it turns out, is also related to what is called the internal direct product (defined below). We will use this direct product to state the main theorem of this paper and break it down into pieces which can be proved sequentially and put together to form a proof of the entire concept.

The Fundamental Theorem

Theorem 1 (The Fundamental Theorem of Finite Abelian Groups)**.** *Every finite abelian group is a direct product (e.g.* $\mathbb{R} \times \mathbb{R}$ *) of cyclic groups of prime power order (e.g.* $\mathbb{Z}_p \times \mathbb{Z}_q$ *). Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.*

For a group G to be **cyclic**,[1] it must be the case that $\exists a \in G : < a >= G$, where $< a >$ is read as "The group generated by a," and understood to mean "...generated under the operation of the main group, G."

The term "direct product" is somewhat ambiguous and depends upon the context in which it is used. Intuitively speaking, an **external direct product** is a product of groups, commonly referred to as the "cross product," and it might seem more natural to the reader to consider products of vector spaces, i.e. it gives a set of coordinates. This is what many authors cite as simply "a direct product." An **internal direct product**, on the other hand, is essentially a product within a set. In all actuality – as we will see – the definitions are more technical and provide the necessary insight.

Definition 1. *For groups G and H, the* ***External Direct Product*** *is the set of ordered pairs (g, h), denoted $G \times H$, where $G \times H = \{(g, h) \| g \in G, h \in H\}$, and when multiplication is defined as below, $G \times H$ forms a group:*

- $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$*, and*
- $e = (e_1, e_2, ..., e_j)$ *for a product in which there are j factors.*

[1] For further reading on the subject of cyclic groups and their importance in Group Theory, see Gallian, Joseph: *Contemporary Abstract Algebra*, 9th Ed.

What's important to note here is that a typical element from an external direct product should look like the Cartesian coordinates to which we have become accustomed. However, an internal direct product forms a group, as we will now see.

Definition 2. *For a group G with subgroups H and K, G is said to be their* ***Internal Direct Product*** *if, for $h \in H, k \in K$:*

- $H \cap K = \{0\}$
- $hk = kh$, *and*
- $HK = G$

Proof of the Theorem

Being that this theorem is deceptively complex and the mathematical concepts it contains are inherently rich, one feels obligated to break it down into smaller pieces in order to effectively impart the ideas within. And, because we are going to use it below, we will now state another theorem.[2]

(Cauchy's Theorem for Abelian Groups) *Let G be a finite abelian group and let p be a prime that divides the order of G. Then G has an element of order p.*

Lemma 1. *Let G be a finite abelian group of order $p^n m$, where p is a prime and $p \nmid m$. Then $G = H \times K$, where $H = \{x \in G | x^{p^n} = e\}$ and $K = \{x \in G | x^m = e\}$. Moreover, $|H| = p^n$*

Proof. Because G is an abelian group, it can be taken for granted that H and K are subgroups. If that's not clear, note that the commutativity ensures that the inverses exist for the elements in each set, thus giving way for the identity to be in each, and because each set consists of elements with finite order, we are closed under operation. Therefore, we must necessarily show only that $G = HK$ and $H \cap K = \{e\}$.

Since $p \not| m$, we have that $gcd(m, p^n) = 1$. This – by Bezout's Identity (or Lemma), given below – tells us that there are integers s and t such that

[2] Gallian, Joseph: *Contemporary Abstract Algebra*, 9th Ed.

$sm + tp^n = 1$. For any $x \in G$, we have that $x = x^1 = x^{sm+tp^n} = x^{sm}x^{tp^n}$. This is by Lagrange, which we will use several times again throughout. Because of the fact that *any* element $x \in G$ can be written as above, we know we are considering all of G when we do so. There are two cases to consider after that: either $x \in H$, or $x \in K$. If x happens to be in H, then x^{tp^n} is going to be the identity, whereas if x happens to be in K, x^{sm} gives the identity. Thus, $x^{sm} \in H$ and $x^{tp^n} \in K$. This is really important for the reader to understand. It can take some intuition and background knowledge to come to the conclusion. The key piece of information comes from Bezout's Lemma which guarantees that: for $a, b \in \mathbf{Z}, \exists s, t \in \mathbf{Z} \| as + bt = gcd(a, b)$. In our proof, we've used the fact that $gcd(p^n, m) = 1$, which allows us to "cycle" back around to the identity element at convenient places (i.e. such that multiples of an element in G can be conveniently found in H or K. Combine all of this with the fact that $|G| = p^n m$, and this means that $x^{sm} \in H$ and $x^{p^n} \in K$.Thus, $G = HK$.

Now, suppose that there exists some $x \in H \cap K$. Then $x^{p^n} = e = x^m$, and then we know that $|x|$ divides both p^n and m.. Since $gcd(p, m) = 1$, $|x| = 1$, which means that $x = e$, and thus, $H \cap K = \{e\}$.

Now, the second thing stated in the lemma above is that $|H| = p^n$. Note that $p^n m = |G| = |HK| = |H||K|/|H \cap K| = |H||K|$. This is because for two finite subgroups H and K of a group, the set $HK = \{hk \| h \in H, k \in K\}$ and $|HK| = |H||K|/|H \cap K|$. Since we've already found that $H \cap K = \{e\}$, we then conclude the statement above.
Then, using Cauchy's Theorem for Abelian Groups, we say that p does not divide $|K|$, so it must divide $|H|$. Therefore $|H| = p^n$. □

If it's still not clear why this is the case, perhaps it is necessary to state Sylow's First Theorem[3] here, since we will also be using it below in Lemma 2.

(Sylow's First Theorem) *If G is a finite group and p is a prime such that p^k divides $|G|$, then G has at least one subgroup of order p^k.*

What this theorem tells us about the lemma above, is that since p^n divides $|G|$, there *necessarily* must be a subgroup of G with order p^n. And since p doesn't divide $|K|$, we have that p divides $|H|$, telling us that H must be that subgroup guaranteed by Sylow.

[3]Gallian, Joseph: *Contemporary Abstract Algebra*, 9th Ed.

What we showed in the above proof is that, if we have an abelian group G, where the order of G finite, but essentially arbitrary, we can break it down into a product of a subgroups H with prime-power order, and K, where $|K|$ isn't initially important, other than it doesn't share a factor with $|H|$. We then conclude fairly simply through induction that this can be done until the orders of the subgroups can no longer be broken down (i.e. they're now all prime-powered subgroups of G. We state our findings in a manner that's more mathematically precise: Given an abelian group G with $|G| = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$, with all the p's being distinct primes, we let $G(p_i)$ denote the set $\{x \in G \| x^{p_i^{n_i}} = e\}$. We then conclude that $G = G(p_1) \times G(p_2) \times ... \times G(p_k)$ and $|G(p_i)| = p_i^{n_i}$.

Lemma 2. *Let G be an abelian group of prime-power order, p^n, and let a be an element of maximum order in G. Then G can be written in the form $< a > \times K$. That is, $G \cong < a > \times K$.*

Proof. Since G is of order p^n for some prime p and some integer n, we know (by Lagrange) that elements in G must have orders that divide said prime power and thus must be of order p^k such that $k \leq n$. At the risk of being redundant, Cauchy and Sylow can give us the existence of such elements and their relative subgroups within G. Cauchy says that if G is a finite abelian group and p is a prime that divides $|G|$, then G has an element of order p. Sylow then says that if G is a finite group and p is a prime such that p^k divides $|G|$, then G has at least one subgroup of order p^k.

We then choose an element $a \in G$ such that a is of maximum order within G. As above, we know by Lagrange that $|a|$ divides $|G|$ and we generate a group with a. Thus, $< a >$ has order p^k, where $k \leq n$. However, if $k = n$, then we can see that $G = < a >$, and we're done. So we will only consider the case when $k < n$.
Now consider division of these group orders – that is, $|G|/| < a > |$. This is

$$p^n / p^k = p^{n-k}.$$

And note that – by Sylow, again – since p^{n-k} divides the order of G, there must necessarily exist a subgroup of order p^{n-k}. Call it H. Since G is abelian, to show the isomorphism $G \cong < a > \times H$, we only need to show that $G = < a > \cdot H$, and $< a > \cap H = \{e\}$.
Because of the fact that we want $< a > \cap H = \{e\}$, we'll only consider a set of such subgroups $K \subset G$ and work from there to find H. Choose the subgroup of maximum order in K and call it H. The requirement for

maximum order will become clear later. For now, though, we have chosen a group that has a trivial intersection with $< a >$, by definition.
Now, suppose that $G \neq < a > \cdot H$. Then there exists some $y \in G$ such that $y \notin < a > \cdot H$. Now let r be the smallest number such that $y^{p^r} \in < a > \cdot H$. Since the max order of elements in G is p^k and $r < k$, then

$$y^{p^k} = e \in < a > \cdot H$$

Let $x = y^{p^{r-1}}$. Since r was the smallest number such that y^{p^r} was in the product, x is not in the product. However, $x^p = (y^{p^{r-1}})^p = y^{p^r} \in < a > \cdot H$. So there exists an $x \in G$ such that $x \notin < a > \cdot H$, but $x^p \in < a > \cdot H$. Let $x^p = a^q h$ such that $q \in \mathbb{Z}$, and $h \in H$. Again, since the max order of elements in G is p^k, then

$$e = x^{p^k} = (x^p)^{p^{k-1}} = (a^q h)^{p^{k-1}} = a^{qp^{k-1}} h^{p^{k-1}}$$

Since $e = a^{qp^{k-1}} h^{p^{k-1}}$, we can conclude that $a^{qp^{k-1}} = h^{-p^{k-1}} \in H$. But $a^{qp^{k-1}} \in < a >$, which implies that $a^{qp^{k-1}} \in < a > \cap H = \{e\}$. Thus, $a^{qp^{k-1}} = e$ and implies $| < a > |$ divides $|a^{qp^{k-1}}|$, so p^k divides qp^{k-1}, which implies that $p|q$. Let $q = ps$, for some $s \in \mathbb{Z}$. With $x \notin < a > \cdot H$, $xa^{-s} \notin H$. But,

$$(xa^{-s})^p = x^p a^{-ps} = x^p a^{-q}$$

Since $x^p \in < a > \cdot H$, $x^p a^{-q} = h$ for some $h \in H$.

Suppose that $K =< xa^{-s} > \cdot H$. Then $< xa^{-s} > \subset K$, which implies that $xa^{-s} \in K$. But $xa^{-s} \notin H$, so $H \neq K$. Therefore, since H has max order, then $< a > \cap K \neq \{e\}$. Let $b \in < a > \cap K$, where $b \neq e$. Then $b =< a > \cap < xa^{-s} > \cdot H$ and there exists $t, u \in \mathbb{Z}$ and $h' \in H$ such that $b = a^t = (xa^{-s})^u h'$. Lets claim that p does not divide u. Suppose it does, then $u = pv$ for some $v \in \mathbb{Z}$. That would mean

$$b = (xa^{-s})^u h' = (xa^{-s})^{pv} h' = ((xa^{-s})^p)^v h'$$

Since we have already found that $x^p a^{-q} \in H$, then $((xa^{-s})^p)^v h' \in H$. Therefore, $b \in H$. But, $b \in < a >$, so $b \in < a > \cap H = \{e\}$. This is a contradiction since $b \neq e$. Thus, p does not divide u. Given that p is a prime and p does not divide u, then $gcd(p, u) = 1$. Again, by Bezouts Identity, there exists integers w and d such that $pw + ud = 1$. Therefore, $x = x^1 = x^{pw+ud} = (x^p)^w (x^u)^d$ Since $x^p \in < a > \cdot H$, then $(x^p)^w \in < a > \cdot H$. Now given it was found that $b = e$,

$$b = a^t = (xa^{-s})^u h' = x^u a^{-su} h' = e$$

So, $x^u = (a^{su}h')^{-1} \in < a > \cdot H$. Therefore, $(x^u)^d \in < a > \cdot H$. So, $x = (x^p)^w(x^u)^d \in < a > \cdot H$, which is a contradiction by how x was originally chosen. Thus, $G = < a > \cdot H$ and $G \cong < a > \times H$
We can consequently apply this method to H to get $H \cong < a_1 > \times H_1$ for some $a_1 \in H$. We continue this until the the product of all cyclic subgroups orders is equal to that of G. Therefore since G is finite and of prime-power order, it can be expressed as an internal direct product of cyclic subgroups of power p. □

Lemma 3. *Every finite abelian group G is uniquely isomorphic to an internal direct product of cyclic groups of prime power order and decomposes into the same number of factors.*

Proof. Let G_1 be a finite abelian group of order p^n . By Lemma 1 and 2, $G_1 = H_1 \times H_2 \times \cdots \times H_r$ where each H_i is cyclic, nontrivial, and of prime-power order. Now let $|H_1| \geq |H_2| \geq \cdots \geq |H_r|$ to accommodate reordering. So,

$$|H_1| = p_1^{n_1}, |H_2| = p_2^{n_2}, \ldots, |H_r| = p_r^{n_r}$$

Now, let $G_2 = \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \ldots \mathbb{Z}_{p_r^{n_r}}$ such that $|\mathbb{Z}_{p_1^{n_1}}| \geq |\mathbb{Z}_{p_2^{n_2}}| \geq \cdots \geq |\mathbb{Z}_{p_r^{n_r}}|$. By definition, the order of a group $\mathbb{Z}_n$ is equal to n. So, $|\mathbb{Z}_{p_1^{n_1}}| = p_1^{n_1}$ and $|H_1| = |\mathbb{Z}_{p_1^{n_1}}|$. Consequently, $|H_2| = |\mathbb{Z}_{p_2^{n_2}}|, \ldots, |H_r| = |\mathbb{Z}_{p_r^{n_r}}|$. Therefore, G_1 and G_2 decompose into the same number of factors, r, and $|H_i| = |\mathbb{Z}_{p_i^{n_i}}|$. Since both are cyclic and of the same order, then $H_i \cong \mathbb{Z}_{pi^{n_i}}$. This implies that $G_1 \cong G_2$, and $|G_1| = |G_2| = p_1^{n_1}p_2^{n_2}...p_r^{n_r}$ where each p_i is distinct. So G_1 is uniquely isomorphic to an internal direct product of cyclic groups of prime power order. □

Thus, we have proved that every finite abelian group is the direct product of cyclic groups of prime-power order, and the decomposition of the group product is unique up to reordering of the factors. Lemma 1 showed that we could **start** the decomposition, Lemma 2 showed that we could **continue** it inductively, and lemma 3 showed that we would end up with a unique factorization. However, as this was quite a long proof, we will now proceed with some examples.

Example 1. *Let $G = U(24) = \{1, 5, 7, 11, 13, 17, 19, 23\}$.*

The above notation, $G = U(24)$ can be read as "the group of invertible elements mod 24," and will be used in this example and the next. Since G

has order 8, then it is isomorphic to one of the following three options,

$$\mathbb{Z}_8$$

$$\mathbb{Z}_4 \times \mathbb{Z}_2$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

The following table shows the elements and their order:

Element	1	5	7	11	13	17	19	23
Order	1	2	2	2	2	2	2	2

Now by Lemma 1, the order of G can be written as the product of some prime power and an integer m. However, we see that the order of G is just of prime power order 2^3. So we turn our attention to Lemma 2 and examine G as a group of prime power order.

Let a be an element of maximum order in G. So let $< a >=< 5 >$, which has order 2. Since $|G| \neq | < 5 > |$, then $G \neq < 5 >$. Thus, there exists a subgroup H such that $G \cong < 2 > \times H$. By Lemma 2's Sylow preliminary, $|G|/| < 5 > | = (2^3)/(2^1) = (8/2) = 4 = |H|$. So, now we must consider all subgroups $H \in G$ of order less than or equal to 4 such that $< a > \cap H = e$. We know H has order less than or equal to 4 since each subgroup can be decomposed into smaller groups of prime power order. We can now apply Lemma 2 to H. So, let b be an element of maximum order in such subgroups H. Since there does not exist an element of order 4 nor 3, let $< b >=< 7 >$ of order 2. Since $|H| \neq | < 8 > |$, then $H \neq < 8 >$ and $H =< b > \times < H_2 >$. Therefore, $|H|/| < 8 > | = (2^2)/(2^1) = (4/2) = 2 = |H_2|$. Now we must consider all subgroups $H_2 \in G$ of order less than or equal to 2 such that $< b > \cap H_2 = \{e\}$. We apply Lemma 2 to H_2. Let c be an element of maximum order in such subgroups H_2. So let $< c >=< 11 >$, which has order 2. Since, $|H_2| = | < c > |$ then $H_2 =< c >$ and we're done with this step. Therefore,

$$G \cong < a > \times < b > \times < c >=< 5 > \times < 7 > \times < 11 > .$$

Let $p_1^{n_1} = 2^1$. So by Lemma 3,

$$| < 5 > | = 2 = 2^1 = p_1^{n_1}$$

$$|\mathbb{Z}_2| = 2 = 2^1 = p_1^{n_1}$$

$$| < 5 > | = |\mathbb{Z}_2|.$$

Hence by a similar application to $< 7 >$ and $< 11 >$, we see that

$$< 5 > \cong \mathbb{Z}_2$$

$$< 7 > \cong \mathbb{Z}_2.$$

$$< 11 > \cong \mathbb{Z}_2.$$

Therefore, $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 2. *Let* $G = U(21) = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

Since G has order 12, then it is isomorphic to one of the following two options,

$$\mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$$

$$\mathbb{Z}_6 \times \mathbb{Z}_2 \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

The following table shows the elements and their order:

Element	1	2	4	5	8	10	11	13	16	17	19	20
Order	1	6	3	6	2	6	6	2	3	6	6	2

Now by Lemma 1, the order of G can be written as the product of some prime power and an integer m_1. So, let $p_1^{n_1} = 3^1$ and $m_1 = 4$. Now, we can decompose m_1 similarly such that it is also the product of some prime power and an integer. Let $m = p_2^{n_2} m_2 = 4$. So, we see that 4 can be written as 2^2. Thus, $|G| = p_1^{n_1} p_2^{n2} = 3^1 * 2^2$. Let A and H be subgroups of G such that their orders are 3^1 and 2^2 respectively. Therefore, $G = A \times H$. We turn our attention to Lemma 2 and examine each subgroup A and H of prime power order.

Let a be an element of maximum order in such subgroups A. Since A has order 3, then we must pick an element in G such that its order is less than or equal to 3. So, let $< a > = < 4 >$. Since $|A| = | < 4 > |$, then $A = < a > = < 4 >$ and we are done with this step. So, now we must consider all subgroups $H \in G$ of order less than or equal to 4. Let b be an element of maximum order in such subgroups H such that $< b > \cap H = \{e\}$. There does not exist an element of order 4 and the group generated by the element of order 3 ($< 16 >$) is the same as $< a >$. By Lemma 1, we see that $A \cap H = \{e\}$, so H does not have an intersection of only the set {e} if

this second group of order 3 is chosen. Then were left with groups of order 2. We can now apply Lemma 2 to H. So, let $< b >=< 8 >$, which has order 2. Since $|H| \neq | < 8 > |$, then $H \neq < 8 >$ and $H =< b > \times < H_2 >$. Therefore, $|H|/| < 8 > | = (2^2)/(2^1) = (4/2) = 2 = |H_2|$. Now we must consider all subgroups $H_2 \in G$ of order less than or equal to 2 such that $< b > \cap H_2 = \{e\}$. We apply Lemma 2 to H_2. Let c be an element of maximum order in such subgroups H_2. So let $< c >=< 13 >$, which has order 2. Since, $|H_2| = | < c > |$ then $H_2 =< c >$ and we're done with this step. Therefore,

$$G \cong < a > \times < b > \times < c >=< 4 > \times < 8 > \times < 13 > .$$

Let $p_1^{n_1} = 3^1$. So by Lemma 3,

$$| < 4 > | = 3 = 3^1 = p_1^{n_1}$$

$$|\mathbb{Z}_3| = 3 = 3^1 = p_1^{n_1}$$

$$| < 4 > | = |\mathbb{Z}_3|.$$

Hence by a similar application to $< 8 >$ and $< 13 >$, we see that

$$< 4 > \cong \mathbb{Z}_3$$

$$< 8 > \cong \mathbb{Z}_2.$$

$$< 13 > \cong \mathbb{Z}_2.$$

Therefore, $G \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 3. *(Alternate Approach) Let* $G = U(21) = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

Since G has order 12, then it is isomorphic to one of the following two options,

$$\mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$$

$$\mathbb{Z}_6 \times \mathbb{Z}_2 \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Now by Lemma 1, the order of G can be written as the product of some prime power and an integer m such that $12 = p^n m = 2^2 * 3$. However, as seen in Lemma 1, G can be decomposed into subgroups of order $p^n m$; i.e. $G = H \times K$ such that $H = p_1^{n_1}$ and $K = p_2^{n_2} m_1 = p_2^{n_2} p_3^{n_3}$. So, we turn our attention to Lemma 2.

Let a be an element of maximum order in G (refer to the table in Ex. 2). So, let $< a >=< 2 >$, which has order 6. Since $|G| \neq | < 2 > |$, then $G \neq< 2 >$. Thus, there exists a subgroup H such that $G \cong< 2 > \times H$. By Lemma 2's Sylow preliminary, $|G|/| < 2 > | = (2^2 * 3^1)/(2^1 * 3^1) = (12/6) = 2 = |H|$. So, now we must consider all subgroups $H \in G$ of order less than or equal to 2 such that $< a > \cap H = \{e\}$. We can now apply Lemma 2 to H. So, let b be an element of maximum order in such subgroups H. So, let $< b >=< 8 >$ of order 2. Since, $|H| = | < b > |$ then $H =< b >$ and we're done with this step. Therefore,

$$G \cong< a > \times < b >=< 2 > \times < 8 > .$$

Let $p_1^{n_1} p_2^{n_2} = 2^1 * 3^1$. So by Lemma 3,

$$| < 2 > | = 6 = 2^1 * 3^1 = p_1^{n_1} p_2^{n_2}$$

$$|\mathbb{Z}_6| = 6 = 2^1 * 3^1 = p_1^{n_1} p_2^{n_2}$$

$$| < 2 > | = |\mathbb{Z}_6|.$$

Hence by a similar application to $< 8 >$, we see that

$$< 2 >\cong \mathbb{Z}_6$$

$$< 8 >\cong \mathbb{Z}_2.$$

Therefore, $G \cong \mathbb{Z}_6 \times \mathbb{Z}_2$ and $\mathbb{Z}_6 \times \mathbb{Z}_2 \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ by our previous result.

References

[1] Joseph Gallian *Contemporary Abstract Algebra, 9th Ed* 2016.

[2] Weisstein Eric W. *"Modulo Multiplication Group"* From MathWorld A Wolfram Web Resource. http://mathworld.wolfram.com/ModuloMultiplicationGroup.html

[3] Monica Agana *Fundamental Theorem of Finite Abelian Groups* http://diamond.boisestate.edu/ liljanab/MATH508/Groups.pdf

[4] csus.edu *Finite Abelian Groups* http://www.csus.edu/indiv/e/elcek/m210a/finiteabelian.pdf