Decomposing U_{438} Into the Product of its Cyclic Subgroups

Robin Martin van den Berg[1]

17 May 2022

Submitted in partial fulfillment of the requirements for the course
SCIMATH302 - Advanced Mathematics: Abstract Algebra
Instructed by Prof. Dr. L.R. van den Doel
during the Spring Semester of 2022
in the Department of Science
of University College Roosevelt, Utrecht University

[1] r.vandenberg@ucr.nl

Contents

List of Tables

1 Introduction

The Fundamental Theorem of Finite Abelian Groups states that every finite Abelian group can be decomposed into a direct product of its cyclic subgroups (Hernstein, 1999). This short paper provides a short introduction to the theorem, as well as a tutorial application of the theorem to the finite Abelian group U_{438}, which is of order 144. The computer program *Wolfram Mathematica* - or *Mathematica* - is used to generate the group U_{438}, many of its subgroups, as well as perform operations on elements in these groups. Section 2 of this tutorial provides a brief outline of the Fundamental Theorem of Finite Abelian Groups. Section 3 provides a brief overview of the group U_{438}. Section 4 details the application of the theorem to U_{438}, and Section 5 provides a brief discussion and conclusion.

2 The Fundamental Theorem of Finite Abelian Groups

The Fundamental Theorem of Finite Abelian Groups states that a finite Abelian group can be decomposed into a product of its cyclic subgroups (Hernstein, 1999). Much of the outline of the proof provided below is based on van den Doel (2017).

2.1 Part 1:

We begin by first considering some finite Abelian group G which has an order $|G| = m * n$, where $GCD(m, n) = 1$ - i.e. m and n are relatively prime. We then define 2 subgroups of G, called M and N, which contain all the elements of G that are of order m and n respectively. Formally, M and N are defined as:

$$M = \{x \in G \mid x^m = e \text{ ; such that : } o(x) = m\} \tag{1}$$

$$N = \{y \in G \mid y^n = e \text{ ; such that : } o(y) = n\} \tag{2}$$

It is easy to show that these are indeed valid subgroups of G. By Cauchy's theorem, since M can be completely generated by some element of order m and N can be completely generated by some element of order n, then we have that $|M| = m$ and $|N| = n$.

We now consider the intersection of the 2 subgroups M and N given by $M \cap N$. We know that $M \cap N$ is a subgroup of both M and N. By Lagrange's Theorem, we know that the order of a subgroup must divide the order of its group, which means that $|M \cap N|$ divides

$|M| = m$ and $|M \cap N|$ divides $|N| = n$. However, since $GCD(m, n) = 1$, we know that the largest possible integer that divides m and n is 1, thus $|M \cap N| = 1$. However, any subgroup with order 1 must be the arbitrary subgroup $\{e\}$, and thus $M \cap N = \{e\}$.

Now we can consider the product of these 2 subgroups MN, and try to determine its elements. We can define this group as:

$$MN = \{x * y \mid x \in M, y \in N\} \tag{3}$$

We begin by taking note of the fact that, since $GCD(m, n) = 1$, there exists some linear combination of m and n that equals 1: $am + bn = 1$ for some a and b. Now consider some element $g \in G$ and write it as: $g = g^1 = g^{am+bn} = g^{am}g^{bn}$. We consider each element of this product, g^{am} and g^{bn}, separately. Raising g^{am} to the power of n gives: $(g^{am})^n = g^{amn} = (g^{mn})^a = (g^{|G|})^a = e^a = e$. This means that g^{am} is an element of G of order n and thus $g^{am} \in N$. Similarly, raising g^{bn} to the power of m gives: $(g^{bn})^m = g^{bmn} = (g^{mn})^b = (g^{|G|})^b = e^b = e$. This means that g^{bn} is an element of G of order m and thus $g^{bn} \in M$. Therefore, $g =$ (some element of order m) $*$ (some element of order n). Therefore, $g \in MN$. Repeating this argument for all $g \in G$ produces the desired result:

$$G = MN = \{g^{am} * g^{bn} \mid g^{bn} \in M \ , \ g^{am} \in N\} \tag{4}$$

This internal direct product can be rewritten as an external direct product:

$$G = M \times N \tag{5}$$

Notice that while the order of the group was taken to be the product of 2 relatively prime numbers m and n, we can also factor the order of the group into the product of primes. For instance, suppose we can factor the order into the product of k primes and their powers, then $|G| = p_1^{j_1} * p_2^{j_2} * ... * p_k^{j_k}$. Setting this equals to m and n produces: $mn = p_1^{j_1} * p_2^{j_2} * ... * p_k^{j_k}$. If we let $m = p_1^{j_1}$ and $n = p_2^{j_2} * ... * p_k^{j_k}$, then we have:

$$|G| = mn = p_1^{j_1} * p_2^{j_2} * ... * p_k^{j_k} = p_1^{j_1} * n; \tag{6}$$

such that $GCD(p_1^{j_1}, n) = 1$. We can drop the subscripts and just write $mn = p^j * n$. This indicates that, the order of a finite Abelian group can be written as the product of: i) a power of a prime $m = p^j$, and ii) a number that must be relatively prime to that power of a prime n.

2.2 Part 2:

We now proceed to the second part of the proof. This part of the proof is the most complex, and as a result only the most import aspects are outlined below. We begin by supposing we have the case outlined above: there is a finite Abelian group G such that $|G| = p^j * n$, where $GCD(p^j, n) = 1$. We suppose the we have some element $a \in G$ that is of maximal order. We can then create the cyclic subgroup generated by this element a, which we denote as $A = (a) = \{a^i \mid \text{for } 0 \leq i < o(a)\}$.

We then consider an element $b \in G$ of order $o(b) = p$ such that $b^p = e$. The cyclic subgroup generated by b is given by $B = (b) = \{b^i \mid \text{for } 0 \leq i < p\}$. We define $b \notin A$ such that $A \cap B = (a) \cap (b) = e$. We can then form the quotient group $G/B = \{Bg \mid \text{for all } g \in G\}$, which is a finite Abelian group in its own right. We then use the element a of maximal order in G to form the co-set $Ba \in G/B$. It can be shown that Ba itself is the element of maximal order in G/B, which produces the cyclic subgroup generated by Ba: (Ba). Forming the quotient group $(G/B)/(Ba)$, we can repeat the argument set out above in this group, as well as the subsequent quotient groups.

This recursive argument continues until it is no longer possible to break down a group into its cyclic subgroups of maximal order, which occurs when the group is itself that cyclic subgroup of maximal order. This produces the result that the finite Abelian group can be written as the product of non-overlapping (besides the unit element) cyclic subgroups. One of these subgroups in the product will be of maximal order such that: $G = A * Q$, where Q represents the other possible products of the other cyclic subgroups.

3 A Finite Abelian Group of Order 144: U_{438}

Before proceeding with an application of the theorem to U_{438}, it is useful to first define the group itself. In order to define U_n, it is necessary to first define $\mathbb{Z}_n$. We can define $\mathbb{Z}_n$ - or $\mathbb{Z}/n\mathbb{Z}$ - as the set of all integers modulo n (for $n > 1$) (Hernstein, 1999). This set forms a group under addition. We express this as:

$$\mathbb{Z}_n = \{[0], [1], ..., [n-1]\} \tag{7}$$

where for some $[a] \in \mathbb{Z}_n$ we define $[a] = \{a + nk \mid k \in \mathbb{Z}\}$. We go on to define U_n as a subset of $\mathbb{Z}_n$. More specifically, U_n is the group of all $[a]$ in $\mathbb{Z}_n$ such that a and n are relatively prime (Hernstein, 1999). Furthermore, U_n forms a subgroup of $\mathbb{Z}_n$ under multiplication. We

express U_n as:

$$U_n = \{[a] \in \mathbb{Z}_n \mid GCD(n, a) = 1\} \tag{8}$$

Therefore, we can see that the groups $\mathbb{Z}_{438}$ and U_{438} are defined as:

$$\mathbb{Z}_{438} = \{[0], [1], ..., [437]\} \tag{9}$$

$$U_{438} = \{[a] \in \mathbb{Z}_{438} \mid GCD(438, a) = 1\} \tag{10}$$

The 144 elements of U_{438} are displayed in the table below:

Table 1: The 144 Elements of U_{438}

[1]	[5]	[7]	[11]	[13]	[17]	[19]	[23]	[25]
[29]	[31]	[35]	[37]	[41]	[43]	[47]	[49]	[53]
[55]	[59]	[61]	[65]	[67]	[71]	[77]	[79]	[83]
[85]	[89]	[91]	[95]	[97]	[101]	[103]	[107]	[109]
[113]	[115]	[119]	[121]	[125]	[127]	[131]	[133]	[137]
[139]	[143]	[145]	[149]	[151]	[155]	[157]	[161]	[163]
[167]	[169]	[173]	[175]	[179]	[181]	[185]	[187]	[191]
[193]	[197]	[199]	[203]	[205]	[209]	[211]	[215]	[217]
[221]	[223]	[227]	[229]	[233]	[235]	[239]	[241]	[245]
[247]	[251]	[253]	[257]	[259]	[263]	[265]	[269]	[271]
[275]	[277]	[281]	[283]	[287]	[289]	[293]	[295]	[299]
[301]	[305]	[307]	[311]	[313]	[317]	[319]	[323]	[325]
[329]	[331]	[335]	[337]	[341]	[343]	[347]	[349]	[353]
[355]	[359]	[361]	[367]	[371]	[373]	[377]	[379]	[383]
[385]	[389]	[391]	[395]	[397]	[401]	[403]	[407]	[409]
[413]	[415]	[419]	[421]	[425]	[427]	[431]	[433]	[437]

Furthermore, the orders of all the elements are displayed below as well:

Table 2: The Orders of All 144 Elements in U_{438}

$o([1]) = 1$	$o([5]) = 72$	$o([7]) = 24$	$o([11]) = 72$	$o([13]) = 72$	$o([17]) = 24$
$o([19]) = 36$	$o([23]) = 36$	$o([25]) = 36$	$o([29]) = 72$	$o([31]) = 72$	$o([35]) = 36$
$o([37]) = 9$	$o([41]) = 18$	$o([43]) = 24$	$o([47]) = 72$	$o([49]) = 12$	$o([53]) = 72$
$o([55]) = 9$	$o([59]) = 72$	$o([61]) = 36$	$o([65]) = 6$	$o([67]) = 36$	$o([71]) = 18$
$o([77]) = 18$	$o([79]) = 36$	$o([83]) = 8$	$o([85]) = 36$	$o([89]) = 18$	$o([91]) = 18$
$o([95]) = 8$	$o([97]) = 12$	$o([101]) = 72$	$o([103]) = 24$	$o([107]) = 72$	$o([109]) = 18$
$o([113]) = 72$	$o([115]) = 72$	$o([119]) = 4$	$o([121]) = 36$	$o([125]) = 24$	$o([127]) = 36$
$o([131]) = 72$	$o([133]) = 72$	$o([137]) = 6$	$o([139]) = 24$	$o([143]) = 12$	$o([145]) = 2$
$o([149]) = 12$	$o([151]) = 72$	$o([155]) = 6$	$o([157]) = 72$	$o([161]) = 72$	$o([163]) = 24$
$o([167]) = 24$	$o([169]) = 36$	$o([173]) = 4$	$o([175]) = 72$	$o([179]) = 72$	$o([181]) = 36$
$o([185]) = 72$	$o([187]) = 18$	$o([191]) = 72$	$o([193]) = 72$	$o([197]) = 8$	$o([199]) = 72$
$o([203]) = 18$	$o([205]) = 72$	$o([209]) = 8$	$o([211]) = 6$	$o([215]) = 18$	$o([217]) = 18$
$o([221]) = 18$	$o([223]) = 9$	$o([227]) = 6$	$o([229]) = 8$	$o([233]) = 72$	$o([235]) = 9$
$o([239]) = 72$	$o([241]) = 8$	$o([245]) = 72$	$o([247]) = 72$	$o([251]) = 18$	$o([253]) = 72$
$o([257]) = 36$	$o([259]) = 72$	$o([263]) = 72$	$o([265]) = 4$	$o([269]) = 36$	$o([271]) = 24$
$o([275]) = 24$	$o([277]) = 72$	$o([281]) = 72$	$o([283]) = 3$	$o([287]) = 72$	$o([289]) = 12$
$o([293]) = 2$	$o([295]) = 12$	$o([299]) = 24$	$o([301]) = 6$	$o([305]) = 72$	$o([307]) = 72$
$o([311]) = 36$	$o([313]) = 24$	$o([317]) = 36$	$o([319]) = 4$	$o([323]) = 72$	$o([325]) = 72$
$o([329]) = 18$	$o([331]) = 72$	$o([335]) = 24$	$o([337]) = 72$	$o([341]) = 12$	$o([343]) = 8$
$o([347]) = 18$	$o([349]) = 18$	$o([353]) = 36$	$o([355]) = 8$	$o([359]) = 36$	$o([361]) = 18$
$o([367]) = 9$	$o([371]) = 36$	$o([373]) = 3$	$o([377]) = 36$	$o([379]) = 72$	$o([383]) = 18$
$o([385]) = 72$	$o([389]) = 12$	$o([391]) = 72$	$o([395]) = 24$	$o([397]) = 9$	$o([401]) = 18$
$o([403]) = 36$	$o([407]) = 72$	$o([409]) = 72$	$o([413]) = 36$	$o([415]) = 36$	$o([419]) = 36$
$o([421]) = 24$	$o([425]) = 72$	$o([427]) = 72$	$o([431]) = 24$	$o([433]) = 72$	$o([437]) = 2$

4 Writing U_{438} as the Direct Product of its Cyclic Subgroups

As a first step, we should decompose $|U_{438}| = 144$ into the product of 2 numbers: a prime (or power of a prime), and a number that is relatively prime to this first prime. We can see that $144 = 16 * 9 = 2^4 * 3^2$.

Before proceeding, it is useful to note that the direct product of a finite Abelian group's

cyclic subgroups can be shown to be isomorphic to one particular direct sum of some other groups of the form $\mathbb{Z}_n$ (van den Doel, 2017). Furthermore, the number of possible direct sums that the direct product could be isomorphic to is given by the prime decomposition of the order of the group. More specifically, it is determined by the number of ways that the powers in this prime decomposition can be partitioned. The powers in $144 = 2^4 * 3^2$ can be partitioned as:

1. $4 = 4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$
2. $2 = 2 = 1 + 1$

Since there are 5 different ways to partition 4, and 2 different ways to partition 2, we can conclude that we can write U_{438} as isomorphic to precisely one of $5 * 2 = 10$ direct sums:

$$U_{438} \simeq \mathbb{Z}_{144} \simeq \begin{cases} \mathbb{Z}_{2^4} \oplus \mathbb{Z}_{3^2} & = & \mathbb{Z}_{16} \oplus \mathbb{Z}_9 \\ \mathbb{Z}_{2^3} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{3^2} & = & \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \\ \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2} & = & \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \\ \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{3^2} & = & \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \\ \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{3^2} & = & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \\ \mathbb{Z}_{2^4} \oplus \mathbb{Z}_{3^1} \oplus \mathbb{Z}_{3^1} & = & \mathbb{Z}_{16} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\ \mathbb{Z}_{2^3} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{3^1} \oplus \mathbb{Z}_{3^1} & = & \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\ \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^1} \oplus \mathbb{Z}_{3^1} & = & \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\ \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{3^1} \oplus \mathbb{Z}_{3^1} & = & \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\ \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{3^1} \oplus \mathbb{Z}_{3^1} & = & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \end{cases} \tag{11}$$

There is a very good reason that we find and describe these direct sums. If we find the direct sum that our direct product is isomorphic to, we can then find out more information about the direct product itself. This is because, the number of groups in the direct sum will be equal to the number of cyclic subgroups in the direct product. Similarly, the orders of the groups in the direct sum will be equal to the orders of the cyclic subgroups in the direct product. In other words, if $\mathbb{Z}_m \oplus \mathbb{Z}_n \simeq ([a]) \times ([b])$, then $|\mathbb{Z}_m| = m = o([a])$ and $|\mathbb{Z}_n| = n = o([b])$ for some $[a], [b] \in U_{438}$. We proceed below by trying to find the direct sum to which our direct product is isomorphic.

The Fundamental Theorem of Finite Abelian Groups states that we can write a U_{438} as the direct product of its cyclic subgroups, where one of these subgroups is a group of

maximal order. As can be seen in Table 2 in the preceding section, the maximal order is 72. However, looking at the direct sums as they are written above, there are clearly no direct sums involving $\mathbb{Z}_{72}$. Therefore, one way of narrowing down our options is to focus on the prime 2 in the product $144 = 2^4 * 9$. We need to look for an element in U_{438} that is of maximal order with respect to the powers of the prime 2. Thus, we should look for elements of order: $2^4 = 16$, or $2^3 = 8$, or $2^2 = 4$, or $2^1 = 2$.

As can be seen in Table 2, there are no elements of order 16. However, there are elements of order 8. Therefore, we can exclude from our list all of the direct sums that include $\mathbb{Z}_{16}$, as well as those that do not include $\mathbb{Z}_8$. This means that we have narrowed down the list to the 2 direct sums: $\mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$ and $\mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$. Before continuing, it is useful to note that the direct sum of groups of the form $\mathbb{Z}_n$ exhibits the following property: $\mathbb{Z}_n \oplus \mathbb{Z}_m = \mathbb{Z}_{n*m}$ iff $GCD(n, m) = 1$. Furthermore, these direct sums commute. Therefore, the 2 direct sums mentioned above can be simplified as:

$$U_{438} \simeq \begin{cases} \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 & \simeq \quad \mathbb{Z}_{72} \oplus \mathbb{Z}_2 \\ \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 & \simeq \quad \mathbb{Z}_{24} \oplus \mathbb{Z}_6 \end{cases} \tag{12}$$

We can consider the first direct sum $\mathbb{Z}_{72} \oplus \mathbb{Z}_2$. From Table 2, we can see that U_{438} contains several elements of order 72 and of order 2. Therefore, we can exclude the second direct sum and conclude that:

$$U_{438} \simeq \mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2 \simeq \mathbb{Z}_{72} \oplus \mathbb{Z}_2 \tag{13}$$

We are now faced with the possibility of writing U_{438} as the direct product isomorphic to $\mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2$, or as the direct product isomorphic to $\mathbb{Z}_{72} \oplus \mathbb{Z}_2$. For completeness, we will do both, starting with the much simpler second case.

4.1 Writing U_{438} as the Direct Product $\simeq \mathbb{Z}_{72} \oplus \mathbb{Z}_2$

Before proceeding to find this direct product, we are faced with the issue of which elements of order 72 and of order 2 should be used to construct the direct product. We make an arbitrary initial choice and select the smallest element of order 72 - [5] - and write its cyclic subgroup below as $([5]) = \{[5]^i \mid 0 \leq i \leq 71\}$:

$$([5]) = \left\{ \begin{array}{cccccccc} [1] & [5] & [11] & [17] & [19] & [25] & [29] & [37] \\ [47] & [49] & [53] & [55] & [59] & [61] & [67] & [79] \\ [83] & [85] & [91] & [95] & [97] & [101] & [107] & [109] \\ [113] & [121] & [125] & [127] & [131] & [145] & [161] & [167] \\ [169] & [179] & [181] & [185] & [187] & [191] & [197] & [209] \\ [211] & [217] & [223] & [233] & [235] & [239] & [245] & [263] \\ [265] & [275] & [281] & [283] & [287] & [289] & [295] & [299] \\ [301] & [305] & [319] & [323] & [335] & [349] & [361] & [367] \\ [373] & [395] & [397] & [403] & [407] & [415] & [425] & [431] \end{array} \right\} \tag{14}$$

With this in mind, we need to find the appropriate element of order 2 to include in the direct product of ([5]), such that the direct product produces U_{438}. Luckily, there are only 3 elements of order 2 in U_{438}: [145], [293], [437]. We can write their cyclic subgroups below as $([a]) = \{[a]^i \mid i = 0, 1 \ , \ a = 145 \ , \ 293 \ , \ 437\}$:

$$([145]) = \{[1], [145]\} \ ; \ ([293]) = \{[1], [293]\} \ ; \ ([437]) = \{[1], [437]\} \tag{15}$$

We can immediately exclude ([145]) from consideration, since ([5]) contains all of the elements from ([145]): both [1] and [145]. Recall that a finite Abelian groups can only be expressed as the direct product of non-overlapping (except for e) cyclic subgroups. That is:

$$([a]) \cap ([b]) = [1] \ , \text{ for } ([a]) \oplus ([b]) = U_n \text{ and } ([a]), ([b]) \subset U_n \tag{16}$$

Therefore, we can use either ([293]) or ([437]) in the direct product. We can conclude that U_{438} can be written as the direct product of 2 cyclic subgroups, one of order 72 - ([5]) - and the other of order 2 - ([293]) or ([437]):

$$U_{438} = ([5]) \times ([293]) = ([5]) \times ([437]) \simeq \mathbb{Z}_{72} \oplus \mathbb{Z}_2 \simeq \mathbb{Z}_{144} \tag{17}$$

These direct products were calculated in *Mathematica*, and compared to the group of U_{438} using a boolean equivalence statement. The simulations confirmed these results:

Table 3: Summary of *Mathematica* Simulations for Equivalence of Direct Products to U_{438}

Direct Product	**Equivalent to U_{438}**
$([5]) \times ([293])$	True
$([5]) \times ([437])$	True

4.2 Writing U_{438} as the Direct Product $\simeq \mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2$

Now, we can also show that:

$$U_{438} \simeq \mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2 \tag{18}$$

by simply following the same process as above. We need to begin by selecting an element of order 9, and element of order 8, and an element of order 2. Arbitrarily, we pick the smallest element of order 9 in U_{438} from Table 2 - [37] - and generate its cyclic subgroup as: $([37]) = \{[37]^i \mid 0 \leq i \leq 8\}$:

$$([37]) = \left\{ \begin{array}{ccc} [1] & [37] & [55] \\ [223] & [235] & [283] \\ [367] & [373] & [397] \end{array} \right\} \tag{19}$$

Now we can consider all of the elements of order 8 in U_{438}. Coincidentally, there are 8 elements of order 8 in U_{438}: [83], [95], [197], [209], [229], [241], [343], and [355]. Fortunately, the cyclic subgroups of order 8 generated by these 8 elements come in only 2 forms. We write them down below in the form: $([a]) = \{[a]^i \mid 0 \leq i \leq 7\}$, where $a =$ 83, 95, 197, 209, 229, 241, 343, or 355:

$$([a]) = \begin{cases} \{[1], [83], [95], [145], [197], [209], [265], [319]\} & \text{if } a = 83, 95, 197, 209 \\ \{[1], [145], [229], [241], [265], [319], [343], [355]\} & \text{if } a = 229, 241, 343, 355 \end{cases} \tag{20}$$

These subgroups have no intersection with ([37]) - the chosen cyclic subgroup of order 9 - and so any one of them could qualify as a suitable candidate for the direct product. We arbitrarily choose, again, the smallest element of order 8 - (8) and use its cyclic subgroup. All that is left is to determine the cyclic subgroup of order 2. Of the 3 cyclic subgroups of order 2 that were established in the previous subsection, only ([145]) must be excluded

(again) - as it it shares [145] in common with all the cyclic subgroups of order 8 above. We proceed by choosing ([437]). Therefore, we can conclude that U_{438} is equal to the product of 3 of its cyclic subgroups - one of order 9, one of order 8 and one of order 2:

$$U_{438} = ([37]) \times ([83]) \times ([437]) \simeq \mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2 \simeq \mathbb{Z}_{144} \tag{21}$$

Constructing the direct product of these 3 cyclic subgroups in *Mathematica* and testing their equivalence to U_{438} again confirms our conclusion stated above.

5 Extra: Finding the Isomorphism

As an extra point of discussion, it is interesting to consider the isomorphism that maps U_{438} onto $\mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2$. Finding this isomorphism explicitly is quite challenging. Therefore, we can rather consider the reverse isomporhism that maps $\mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2$ onto U_{438}. We can then define the desired isomorphism as the inverse of this isomorphism. We begin by defining the homomorphism $\phi : \mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2 \to U_{438}$ as:

$$\phi([a]_9, [b]_8, [c]_2) = [37^a \times 83^b \times 437^c]_{438} \tag{22}$$

where $[]_n$ indicates an equivalence class modulo n. In order to check if this homomorphism is well defined, we should investigate whether the defining property of homomorphisms hold in this case: $\phi(x * y) = \phi(x) *' \phi(y)$, where $*$ is the operation of the group in the domain and $*'$ is the operation of the group in the co-domain. Since $\mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2$ forms a group under addition and U_{438} forms a group under multiplication, we know that $* = +$ and $*' = \times$. This means that we need $\phi(x + y) = \phi(x) \times \phi(y)$.

We consider the image under ϕ of another element from the direct sum: $\phi([d]_9, [e]_8, [f]_2) = [37^d \times 83^e \times 437^f]_{438}$. Therefore, for ϕ to be a valid homomorphism, we need $\phi\Big(([a]_9, [b]_8, [c]_2) + ([d]_9, [e]_8, [f]_2)\Big) = \phi([a]_9, [b]_8, [c]_2) \times \phi([d]_9, [e]_8, [f]_2)$. We consider the first part, where we have that: $\phi\Big(([a]_9, [b]_8, [c]_2) + ([d]_9, [e]_8, [f]_2)\Big) = \phi\Big(([a+d]_9, [b+e]_8, [c+f]_2)\Big)$ which is given by:

$$\phi\left(([a]_9, [b]_8, [c]_2) + ([d]_9, [e]_8, [f]_2)\right) = [37^{a+d} \times 83^{b+e} \times 437^{c+f}]_{438} \tag{23}$$

We should now compare this to $\phi([a]_9, [b]_8, [c]_2) * \phi([d]_9, [e]_8, [f]_2)$ which is given by:

$$\phi([a]_9, [b]_8, [c]_2) \times \phi([d]_9, [e]_8, [f]_2) = [37^a \times 83^b \times 437^c]_{438} \times [37^d \times 83^e \times 437^f]_{438} \tag{24}$$

$$\phi([a]_9, [b]_8, [c]_2) \times \phi([d]_9, [e]_8, [f]_2) = [37^{a+d} \times 83^{b+e} \times 437^{c+f}]_{438} \tag{25}$$

Therefore: $\phi\Big(([a]_9, [b]_8, [c]_2) + ([d]_9, [e]_8, [f]_2)\Big) = \phi([a]_9, [b]_8, [c]_2) \times \phi([d]_9, [e]_8, [f]_2)$. This means that ϕ is indeed a valid homomorphism. We can now investigate whether or not this homomorphism is 1-1. To do this, it is useful to consider the kernel of ϕ given by $Ker(\phi) = \{([a]_9, [b]_8, [c]_2) \in \mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2 \mid \text{for all } \phi([a]_9, [b]_8, [c]_2) = [1]_{438}\}$. It is clear that the product $37^a * 83^b * 437^c$ only evaluates to 1 when $a, b, c = 0$ such that $37^0 * 83^0 * 437^0 = 1 * 1 * 1 = 1$. Therefore, $Ker(\phi) = \{([0]_9, [0]_8, [0]_2)\}$ and $|Ker(\phi)| = 1$. Therefore, the homomorphism is indeed 1-1.

Furthermore, we can consider whether or not the homomorphism is onto. We can first consider the order of $\mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2$. Since $\mathbb{Z}_9$ has 9 elements, $\mathbb{Z}_8$ has 8 elements, and $\mathbb{Z}_2$ has 2 elements, we have that there are $9 * 8 * 2 = 144$ possible ways to form a direct sum consisting of 1 class from each group. Similarly, we already know that the order of U_{438} is 144. Since the orders of the 2 groups are equal, and ϕ has already been shown to be a valid 1-1 homomorphism from $\mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2$ to U_{438}, we know that ϕ must be an isomorphism. Lastly, we can define the isomorphism $\theta : U_{438} \to \mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2$ as $\theta = \phi^{-1}$.

6 Discussion and Conclusion

This paper has provided a brief overview of the Fundamental Theorem of Finite Abelian groups, as well as a tutorial of its application to U_{438}. However, this paper serves only as a brief introduction to the theorem and its applications. Future research papers can aim to cover the full proof of the theorem in greater depth. Furthermore, this paper did not discuss the isomorphism from U_{438} onto the direct products in full detail. This could also be a topic for future research papers. Nevertheless, this paper does provide a good introduction to why a finite Abelian group can be decomposed into the product of cyclic subgroups, and how knowing this alone can be quite illuminating when applied to a specific Abelian group.

References

Herstein, I.N. (1999). Abstract algebra (3rd ed.). J. Wiley & Sons.
van den Doel, L.R. (2017). SCI 312 - Finite Abelian Groups [PDF]. University College Roosevelt.