On The Non-kth Elements of a Group

Brett Grimes
Carthage College
bgrimes@carthage.edu

April 10, 2017

Abstract

In Abstract Algebra, raising an element to a certain power can provide insight on various properties of both the element itself and the group it is a part of. This thesis is interested in the number of elements of a group that cannot be represented as a fixed power of any element in the group. Interesting patterns emerge when we compare such values for non-isomorphic groups of the same order. Specifically, we compare the group of Integers Modulo $2n$ and the corresponding Dihedral group with the same order. We then expand to more general cases of direct and semidirect products.

1 Introduction

This thesis is a continuation of research with many previous contributors. The history of this particular area of research is brief but far reaching. The first published research involving non-kth elements (see Definitions 1 & 2 for a detailed description) was a collaboration of five mathematicians working in four different countries: E. Bannai (United States), M. Denza and P. Frankl (France), A.C. Kim (South Korea), and M. Kiyota (Japan). Their paper, published in 1989 entitled "On the Number of Elements Which Are Not n-th Powers in a Finite Group", proved the existence of a lower bound on the number of elements which fail to be a n-th power where $n > 1$ is a divisor of the order of the group. Specifically, this lower bound happens to be the square root of the number of elements in the group.

In 2015, a paper with a similar title was written by W. Cocke, I.M. Isaacs, and D. Skabelund. Their paper attempts to derive as much information as possible about a group given that it has a finite, non-zero number of elements that are not kth powers in a group. They are able to provide sufficient conditions that G is in fact finite. However, they are unable to prove that this guarantees G to be finite in all cases. Very recently, in February 2017, S.V. Ivanov provided a counter-example showing that a proof would be impossible.

A student of Isaacs, Sara Jensen, also began investigating the set of non-kth elements. Her research focused on the sequence of elements in G which cannot

be represented as a kth power. One result of hers is a proof that such a sequence determines the group G when$G$ is a finite Abelian group. In other words, this sequence is unique for finite Abelian groups. She is now attempting to generalize this result to other categories of groups, specifically nilpotent groups. This thesis was written in collaboration with Jensen.

2 Definitions and Development

We begin by formally defining what we mean by "non-kth elements".

Definition 1. Let G be a possibly infinite group, and fix an integer $k > 0$. We define the set G^k as follows:

$$G^k = \{x^k \mid x \in G\}.$$

Example 2. Let G be a finite group and let k be the **exponent** (least common multiple of the orders of each element in G) of the group. In this case, every element is mapped to the identity when raised to the kth power. Thus, $G^k = \{e\}$.

The previous example is helpful in understanding how we might think about this process. For finite groups, we can think of a function (or mapping) from G to G that raises every element of G to a power k. Thus, G^k is the image of this function. Also note how we are now provided with an lower bound for $|G^k|$ as the identity never changes when raised to a power.

Example 3. If k is coprime to the order of G, then $G^k = G$.

Proof. It is again helpful to this of this as a mapping. Let $\phi(x)$ map $x \to x^k$ where k is coprime to $|G|$. Because $|ker(\phi)| = 1$, we know that ϕ is a bijection. □

In this paper we are interested in the complement of the set G^k, as defined below.

Definition 4. Let G be a possibly infinite group, and fix and integer $k > 0$. We write

$$N_k(G) = G - G^k$$

and

$$n_k(G) = |G| - |G^k|.$$

This is the notation used by Bannai and Isaacs. To summarize, $N_k(G)$ is the set of non-kth powers in G and $n_k(G)$ is the number of such elements. In some instances, we may want to talk about the set (or sequence) of values for all $k \in \mathbb{N}$. In that case, we will use $n_i(G)$ to denote the set (or sequence) of $n_k(G)$ values $k > 0$. The meaning should be clear within the context of its use.

The following definitions and examples will be helpful in following the proofs in the Results section.

Definition 5. Given any number n and a prime number p, the ***p*-part** of n is the greatest power of p that divides n.

Example 6. The 2-part of 28 is $2^2 = 4$.

The following example will walk through the computation process of the number of non-kth elements for a specific group.

Example 7. Let $G = \mathbb{Z}_{12}$. We will compute $|G^k|$ for various values of k. When k is a divisor of $|G|$, it is sufficient to count the number of multiples of k in G. That is, for $k = 3$, we need only to count the number of multiples of 3 (including 0), so $|G^3| = 4$. When k is coprime to G, we know from the example above that $|G^k| = 12$. However, how do we compute $|G^9|$? Consider the isomorphism $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3$. We can now work component-wise. Because 9 is coprime to 4 and a multiple of 3, we have 4 choices in the first component and only 1 choice (the identity) in the second. Thus, $|G^9| = 4$. To verify this we can perform the mapping $G \to G^k$ by $x \to x^k$. When we do this we obtain $G^9 = \{0, 9, 6, 3\}$. Notice that this set is equal to G^3. This remains true in general. That is, if k_0 is not coprime to $|G|$ then $G^{k_0} = G^{k_1}$ for some divisor k_1 of $|G|$. Therefore, when comparing groups, we need only consider the values of k that divide the order of the groups.

Example 8. In this example we will examine two groups that have:

- the same order,
- different exponents, and
- orders with same number of divisors.

Two such groups are $G_1 = \mathbb{Z}_4 \oplus \mathbb{Z}_4$ and $G_2 = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. The tables below show the breakdown of each group. The middle columns represent the number of choices for elements that can be expressed as some element in the respective group in the direct product, using the methods described in Example 7. For example, if $k = 2$ we have two choices in $\mathbb{Z}_4$, because $4 = 2^2 = 2 + 2$ and $2 = 1^2 = 1 + 1$. Recall that in the integers modulo n, the operation is addition. Thus, G_1^k has $2 * 2$ elements.

k	$\lvert G_1^k \rvert$	$n_k(G_1)$
1	$4 \cdot 4$	0
2	$2 \cdot 2$	12
4	$1 \cdot 1$	15
8	$1 \cdot 1$	15
16	$1 \cdot 1$	15

k	$\lvert G_2^k \rvert$	$n_k(G_2)$
1	$4 \cdot 2 \cdot 2$	0
2	$2 \cdot 1 \cdot 1$	14
4	$1 \cdot 1 \cdot 1$	15
8	$1 \cdot 1 \cdot 1$	15
16	$1 \cdot 1 \cdot 1$	15

We have the sets $n_i(G_1) = \{0, 12, 15\}$ and $n_i(G_2) = \{0, 14, 15\}$, which are not equal. Note that the 2-part of $|G^k|$ is equal to the 2-part of $n_k(G)$ in both cases. Interested readers are encouraged to work out examples of a larger scale. For example, try $G_1 = \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3$ and $G_2 = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{27}$.

The following is the formal result of Jensen's work as discussed in the Introduction.

Theorem 9. *Suppose G_1 and G_2 are finite Abelian groups and $n_i(G_1) = n_i(G_2)$ for all i. Then $G_1 \cong G_2$.*

In other words, the sequence $n_i(G)$ determines G when G is a finite Abelian group. A proof of this can be found in [1].

3 Results

A goal of this research is to compare different "classes" of groups. We learned that the sequence $n_i(G)$ determines G for finite Abelian groups, but what if we were to compare non-Abelian finite groups and Abelian groups. Could we construct a group that happened to have the same sequence $n_i(G)$? Theorem 9 shows that this is impossible for Dihedral groups and the integers modulo n. Later, we generalize this result to more general semidirect products.

Theorem 10 (Dihedrals vs. Integers)**.** *Given any Dihedral group of order $2n$, and a corresponding group of integers modular $2n$, there exists at least one integer k_0 such that*

$$n_{k_0}(\mathbb{Z}_{2n}) \neq n_{k_0}(D_n).$$

Proof. We begin by defining $n_{k_0}(D_n)$ and $n_{k_0}(\mathbb{Z}_{2n})$ in terms of $|\mathbb{Z}_n^k|$. It has been shown that $n_k(G) = 0$ for any k that is relatively prime to the order of the group, so we will assume going forward that k is a divisor of $2n$.

The structure of Dihedral groups allows us to write $n_{k_0}(D_n)$ as

$$n_{k_0}(D_n) = \begin{cases} |\mathbb{Z}_n^k| & k \text{ is even,} \\ |\mathbb{Z}_n^k| + n & k \text{ is odd.} \end{cases}$$

This, of course, is due to the fact that rotations act like $\mathbb{Z}_n$ and reflections are of order 2, and thus map to the identity when k is even (and map to themselves when k is odd).

It is necessary to split $n_{k_0}(\mathbb{Z}_{2n})$ into two cases, when n is even and when n is odd. Let us first consider the case when n is even. Let a be the 2-part of k and let b be the 2-part of n. It follows from previous results that

$$n_{k_0}(\mathbb{Z}_{2n}) = \begin{cases} 2 * |\mathbb{Z}_n^k| & k \text{ is even and } a \leq b, \\ |\mathbb{Z}_n^k| & k \text{ is even and } b > a, \\ 2 * |\mathbb{Z}_n^k| & k \text{ is odd.} \end{cases}$$

Thus, whenever we have a k such that k is odd or $a > b$ we have $n_k(\mathbb{Z}_{2n}) \neq n_k(D_n)$.

When n is odd we have

$$n_{k_0}(\mathbb{Z}_{2n}) = \begin{cases} |\mathbb{Z}_n^k| & \text{k is even,} \\ 2 * |\mathbb{Z}_n^k| & \text{k is odd.} \end{cases}$$

Thus, whenever k is odd we have $n_k(\mathbb{Z}_{2n}) \neq n_k(D_n)$. We know such a k must exist because n itself is odd.

□

We have the result we wanted, but we will pause to examine some interesting patterns and properties of the relationship between the integers modulo $2n$ and Dihedral groups.

Corollary 11. *Let n be any integer that is not a power of 2. Given any Dihedral group of order $2n$, and a corresponding group of integers modulo $2n$, for any odd divisor k of $2n$, we have*

$$n_k(\mathbb{Z}_{2n}) = 2 * n_k(D_n).$$

Proof. We use the general definitions for both $n_{k_0}(D_n)$ and $n_{k_0}(\mathbb{Z}_{2n})$ from the previously to compute that when k is odd

$$n_k(D_n) = 2n - (|\mathbb{Z}_n^k| + n) = n - |\mathbb{Z}_n^k|.$$

Furthermore, we have

$$\begin{aligned} n_k(\mathbb{Z}_{2n}) &= 2n - 2 * |\mathbb{Z}_n^k| \\ &= 2 * (n - |\mathbb{Z}_n^k|) \\ &= 2 * n_k(D_n). \end{aligned}$$

Thus, whenever k is an odd divisor of $2n$ we have $n_k(\mathbb{Z}_{2n}) = 2 * n_k(D_n)$, as desired. Because n is not a power of 2 we know that such a k exists.

□

Corollary 12. *Let n be any odd integer. Given a Dihedral group of order $2n$ and a corresponding group of integers modular $2n$, for all even divisors k of $2n$ we have*

$$n_k(\mathbb{Z}_{2n}) = n_k(D_n).$$

Proof. This follows directly from 10. We have shown that

$$n_k(D_n) = 2n - |\mathbb{Z}_n^k| = n_k(\mathbb{Z}_{2n}).$$

□

By combining Corollaries 11 and 12 we see that when n is an odd integer, the sequences $n_{k_0}(D_n)$ and $n_{k_0}(\mathbb{Z}_{2n})$ will be identical for all k except when k is an odd divisor of $2n$, in which case $n_k(\mathbb{Z}_{2n}) = 2 * n_k(D_n)$.

Corollary 13. *If n is a power of 2 and $n_i(G)$ denotes the set of $u_k(G)$ values for any $k \in \mathbb{N}$, then the intersection $n_i(D_n) \bigcap n_i(\mathbb{Z}_{2n})$ is the set $\{0, 2n-1\}$.*

Proof. Because the 2-part of all divisors k where $1 < k < 2n$ are less than or equal to the 2-part of n we have

$$n_k(D_n) = 2n - |\mathbb{Z}_n^k| \neq 2n - 2 * |\mathbb{Z}_n^k| = n_k(\mathbb{Z}_{2n}).$$

□

We will now generalize the previous theorem to more general cases of semidirect products. First, we need a definiton of semidirect product.

Definition 14 (Semidirect Product)**.** Given a group G, a subgroup H, and a normal subgroup $N \triangleleft G$, then the following are equivalent.

- The group G is the product of subgroups, $G = NH$, where $N \bigcap H = \{e\}$.
- For every $g \in G$, there are unique $n \in N$ and $h \in H$ such that $g = nh$.
- There exists a homomorphism $G \to H$ that is the identity on H and whose kernel is N.

If these statements hold, we say G is the **semidirect product** of N and H and write this as $G = N \rtimes H$.

Example 15. The Dihedral group of order $2n$ is the semidirect product of cyclic groups of order n and 2. That is, if C_n denotes a cyclic group, then $D_n \cong C_n \rtimes C_2$.

Lemma 16. *Let the semidirect product $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ where p is a prime number and q is coprime to p be given. Then, the order of $g = nh$ where $n \in \mathbb{Z}_p, n \neq e$ and $h \in \mathbb{Z}_q, h \neq e$ is q.*

Proof. Let N denote the normal subgroup $\mathbb{Z}_{p^a}$ in G, and let H denote the (non-normal) subgroup $\mathbb{Z}_q$. We know that $|g| \in \{1, q, p, pq\}$. However, we know that the order of g cannot be 1 or $p^a q$ because it is neither the identity nor a cyclic generator of the entire group. Suppose $|g| = p$. Then, $< nh >$ is a subgroup of order p. We know from Sylow's Third Theorem that there exists only one Sylow p-subgroup, so $< nh >= N$. However, if $nh \in H$, we compute that $n^{-1}nh = h \in H$ which contradicts the definition of semidirect product. Thus, $o(g) = q$. □

Theorem 17 (Powers of p Semidirect Products)**.** *Let G be the group formed by the semidirect product $\mathbb{Z}_{p^a} \rtimes \mathbb{Z}_q$ where p is a prime number and q is coprime to p^a. If G_0 is the group $\mathbb{Z}_{p^a q}$, then*

$$n_{p^i}(G_0) = q * n_{p^i}(G)$$

where i is any natural number.

Proof. Let N denote the normal subgroup $\mathbb{Z}_{p^a}$ in G, and let H denote the (non-normal) subgroup $\mathbb{Z}_q$. Recall that by the definition of semidirect products, we know that for every $g \in G$, there are unique $n \in N$ and $h \in H$ such that $g = nh$. For convenience we break down G into the four following cases

$$A = \{e \cdot e\},$$
$$B = \{n \cdot e \mid n \in N, n \neq e\},$$
$$C = \{e \cdot h \mid h \in H, h \neq e\},$$
$$D = \{n \cdot h \mid n, h \neq e\}.$$

Notice that the union of these sets is the group G and their intersection is the empty set. This allows us to write

$$n_k(G) = |G| - (|A^k| + |B^k| + |C^k| + |D^k|)$$

.

For clarity, it should be noted that while A, B, C are all subgroups of G, D is not a subgroup of G as it does not contain the identity. Therefore, we must define $D^k := \{d^k \mid d \in D\}$. It is not necessary that $d^k \in D$.

The size of the subsets A,B, and C should be obvious to the reader as well as the order of any element in those sets. The size of set D is easily computed, $|D| = (p^a - 1) \cdot (q - 1)$, but the order of an element $d \in D$ may not be as obvious. Jensen has a proof similar to the lemma above which shows that if $g \in D$ then $o(g) = q$. We are able to finish the proof as follows.

g	num. elements	order
$e \cdot e$	1	1
$n \cdot e$	$p^a - 1$	p^k for some $0 \leq k \leq a$
$e \cdot h$	$q - 1$	q
$n \cdot h$	$(p^a - 1)(q - 1)$	q

Let $k = p^i$. We compute that

$$\begin{aligned} n_k(G) &= p^a * q - [(1) + (p^{a-i} - 1) + (q - 1) + ((p^a - 1)(q - 1)) \\ &= p^a * q - (p^{a-i} + p^a * q - p^a) \\ &= p^a - p^{a-i} \\ &= p^{a-i}(p^i - 1). \end{aligned}$$

We compare this to $n_(G_0) = p^{a-i}q(p^i - 1)$ and see that $n_{p^i}(G_0) = q * n_{p^i}(G)$, as desired.

□

4 Further Research

Although we have yet to produce a proof for the general case of any two cyclic groups, we are confident that the results will hold. That is, the sequence $n_i(G)$ determines the group if G is cyclic. One promising method of a proof involves investigating how factor groups hold certain properties when looking at the non-kth elements.

References

[1] Jensen, S., *The Sequence $n_k(G)$ Determines G when G is a Finite Abelian Group*, Carthage College, Kenosha, 2016.

[2] E. Bannai, M. Deza, P. Frankl, A. C. Kim, and M. Kiyota, *On the number of elements which are not nth powers in finite groups,* Comm. Algebra, 1989.