Generalized Conjugacy Classes

Pramod N. Achar*

February 9, 1997

Abstract

Generalized conjugation is the action of a group on its underlying set given by $(g, x) \mapsto \phi(g)xg^{-1}$, where $\phi : G \to G$ is some fixed endomorphism. Here we study combinatorial properties of the sizes of the orbits of the preceding action. In particular, we reduce the problem to a simpler case if ϕ has a nontrivial kernel or if it is an inner automorphism, and we give a construction that allows a partial analysis in the general case.

1 Introduction

1.1 Definition and Motivation

Let $\operatorname{End} G$ denote the semigroup of endomorphisms, and let S_G denote the group of permutations on the underlying set of G. Generalized conjugation associates to each element $\phi \in \operatorname{End} G$ an action $G \to S_G$ of G on its own uderlying set. In particular, if ϕ is the identity endomorphism, the associated action $G \to S_G$ takes $g \in G$ to the permutation which is conjugation by g. The computation of the associated element of S_G for given (ϕ, g) is described below.

Why do we wish to study generalized conjugation? Suppose that G is the fundamental group of some compact 2-manifold X, and that ϕ is induced by some continuous map $f : X \to X$. Consider the orbits in G under the action associated to ϕ (referred to in the literature as "Reidemeister classes"): it turns out that

*Author supported by NSF grant DMS-9322338

the structure of these orbits carries information about the number of fixed points that f has. The reader is referred to [1] for further information on this topic.

DEFINITION 1.1 *To each $\phi \in \operatorname{End} G$, we associate an action $G \to S_G$ by the formula*

$$g * x = \phi(g)xg^{-1}.$$

*This action is called ϕ-**conjugation**; the element $g * x$ is called the ϕ-**conjugate** of x by g. The orbit of x under this action is called the ϕ-**conjugacy class** of x and is denoted C_x^ϕ. The stabilizer of x under this action is called the ϕ-**centralizer** of x and is denoted Z_x^ϕ.*

Note that if we take $\phi = id$, we obtain ordinary conjguation. We now confirm the following crucial fact.

LEMMA 1.2 *ϕ-conjugation is an action of a group G on the underlying set of G.*

Proof. Let us write $g * x = \phi(g)xg^{-1}$. Then we have

$$\begin{aligned} (gh) * x &= \phi(gh)x(gh)^{-1} \\ &= \phi(g)\phi(h)xh^{-1}g^{-1} \\ &= g * (\phi(h)xh^{-1}) \\ &= g * (h * x) \end{aligned}$$

Furthermore,

$$1 * x = \phi(1)x1^{-1} = x,$$

so ϕ-conjugation is in fact an action. $\square$

1.2 Examples

Let us take a look at a few well-known groups and how they split up into generalized conjugacy classes under various endomorphisms.

Group	Endomorphism	Generalized Conjugacy Class Sizes
A_5	id	$[1, 12, 12, 15, 20]$
A_5	$x \mapsto x^{(1\,5\,2)}$	$[1, 12, 12, 15, 20]$
A_5	$x \mapsto x^{(1\,2)}$	$[10, 20, 30]$
D_4	id	$[1, 1, 2, 2, 2]$
D_{20}	$r \mapsto r^{13},\ f \mapsto fr^{10}$	$[5, 5, 10, 10, 10]$
D_{20}	$r \mapsto r^5,\ f \mapsto f$	$[5, 5, 10, 10, 10]$
S_6	id	$[1, 15, 15, 40, 40, 45, 90, 90, 120, 120, 144]$
S_6	τ^*	$[36, 144, 180, 180, 180]$
A_6	id	$[1, 40, 40, 45, 72, 72, 90]$
A_6	$x \mapsto x^{(1\,2)}$	$[15, 15, 90, 120, 120]$
A_6	τ^*	$[36, 72, 72, 90, 90]$
$\mathbb{Z}_{27}$	$x \mapsto x^{10}$	$[3, 3, 3, 3, 3, 3, 3, 3, 3]$
$\mathbb{Z}_{27}$	$x \mapsto x^4$	$[9, 9, 9]$

*See [2] for the construction of an outer automorphism τ of S_6. τ also restricts to give an outer automorphism of A_6.

In the preceding table, notation such as "$x \to x^{(1\,6\,2)}$" denotes the endomorphism given by conjugation by the element $(1\,6\,2)$.

1.3 A Note on Notation

$\operatorname{Aut} G$ is the standard notation for the automorphism group of a group G. Additionally, we shall use $\operatorname{Inn} G$ to denote the normal subgroup of inner automorphisms, and $\operatorname{Out} G$ to denote the quotient $\operatorname{Aut} G / \operatorname{Inn} G$. Each element α of $\operatorname{Inn} G$ is given by conjugation by some element $g \in G$; to denote this, we shall write $\alpha = \operatorname{Ad}_g$. If $G \lhd H$, then conjugation by any element $h \in H$ gives a well-defined (but not necessarily inner) automorphism of G; the Ad_h notation will be used in such cases as well.

Earlier, the notations Z_x^ϕ and C_x^ϕ were introduced for the ϕ-centralizer and the ϕ-conjugacy class of x, respectively. In particular, Z_x^{id} and C_x^{id} will denote the ordinary centralizer and conjugacy class of x. We now also introduce the following:

Definition 1.3 *Let*

$$Z(\phi) = \bigcap_{x \in G} Z_x^{\phi}.$$

This group is called the ϕ**-center** *of the group.*

In particular, $Z(id)$ is the center of the group.

2 Basic Results

2.1 Endomorphisms with Kernels

Consider the example of D_{20} given earlier, with $\phi : D_{20} \to D_{20}$ given by $\phi : r \mapsto r^5,\ f \mapsto f$. This ϕ's image is isomorphic to D_4, and the ϕ-conjugacy class structure looks like a constant multiple (in fact, $|\ker \phi|$) times the id-conjugacy class structure of D_4.

This example suggests that perhaps in general the conjugacy class structure produced by endomorphisms with kernels is some multiple of the conjugacy class structure given by an induced automorphism on some quotient of the original group. That turns out to be true, but the constant multiple is not simply $|\ker \phi|$ in general.

Definition 2.1 *Given an endomorphism* $\phi : G \to G$*, define*

$$\ker^i \phi = \begin{cases} \{1\} & \text{if } i = 0; \\ \phi^{-1}(\ker^{i-1} \phi) & \text{if } i > 0. \end{cases}$$

(Note that $\ker^1 \phi$ *is the same as the ordinary kernel of* ϕ*.) Define*

$$\ker^\infty \phi = \bigcup_{i=0}^{\infty} \ker^i \phi.$$

$\ker^\infty \phi$ *will called the* **iterated kernel** *of* ϕ*.*

Since $\ker^0 \phi$ is a subgroup, and the preimage of any subgroup is a subgroup, it follows that $\ker^i \phi$ is a subgroup of G for all nonnegative integers i. We now establish a few basic properties of the iterated kernel.

Lemma 2.2 *If* $0 \leq i < j$, *then* $\ker^i \phi \subset \ker^j \phi$.

Proof. We shall show by induction that $\ker^i \phi \subset \ker^{i+1} \phi$. First, it is clear that $\ker^1 \phi = \ker \phi$ contains $\ker^0 \phi = \{1\}$. Now, suppose that $\ker^{i-1} \phi \subset \ker^i \phi$. $x \in \ker^i \phi$ implies $\phi(x) \in \ker^{i-1} \phi$, and hence $\phi(x) \in \ker^i \phi$. But that latter condition means precisely that $x \in \ker^{i+1} \phi$. Thus, $\ker^i \phi \subset \ker^{i+1} \phi$. ◻

Lemma 2.3 $\ker^i \phi$ *is a normal subgroup of* G.

Proof. Again, we proceed by induction. $\ker^0 \phi$ is clearly normal. Now, suppose $\ker^{i-1} \phi$ is known to be normal, and take $x \in \ker^i \phi$. For any $g \in G$, we wish to show that $g^{-1}xg \in \ker^i \phi$. Now, $\phi(g^{-1}xg) = \phi(g)^{-1}\phi(x)\phi(g) \in \ker^{i-1} \phi$ because it is a conjugate of $\phi(x) \in \ker^{i-1} \phi$, and $\ker^{i-1} \phi$ is normal. But $\phi(g^{-1}xg) \in \ker^{i-1} \phi$ implies $g^{-1}xg \in \ker^i \phi$, as desired. ◻

Lemma 2.4 $\ker^\infty \phi$ *is a normal subgroup of* G.

Proof. Take $x, y \in \ker^\infty \phi$. x is contained in some $\ker^i \phi$, and y is contained in some $\ker^j \phi$. Take $m = \max\{i, j\}$; then, by Lemma 2.2, $x, y \in \ker^m \phi$. Since $\ker^m \phi$ is a subgroup, $xy \in \ker^m \phi$ and $x^{-1} \in \ker^m \phi$. Therefore, $xy \in \ker^\infty \phi$ and $x^{-1} \in \ker^\infty \phi$. Moreover, for any $g \in G$, $g^{-1}xg \in \ker^m \phi$, and hence $g^{-1}xg \in \ker^\infty \phi$. Thus $\ker^\infty \phi$ is a normal subgroup. ◻

Proposition 2.5 *Given an endomorphism* $\phi : G \to G$, *the induced map* $\phi^{\ker} : G/\ker^\infty \phi \to G/\ker^\infty \phi$ *is an automorphism.*

Proof. We begin by checking that ϕ induces a well-defined map on $G/\ker^\infty \phi$. If x and y are in the same coset of $\ker^\infty \phi$, i.e., if $x = yk$ where $k \in \ker^\infty \phi$, then $\phi(x) = \phi(y)\phi(k)$. We know that $\phi(k) \in \ker^\infty \phi$ also, so $\phi(x)$ and $\phi(y)$ lie in the same coset of $\ker^\infty \phi$. Thus $\phi^{\ker}$ is well-defined.

Next, we check that $\phi^{\ker}$ is injective. Suppose $\phi(x) = \phi(y)z$ for $z \in \ker^\infty \phi$; we wish to show that x and y lie in the same coset of $\ker^\infty \phi$. Now, $\phi(y^{-1}x) = z$, so $y^{-1}x \in \phi^{-1}(\{z\})$. By construction of $\ker^\infty \phi$, this implies that $y^{-1}x \in \ker^\infty \phi$, so in fact x and y are in the same coset.

Finally, we note that in a finite group, an injective endomorphism is necessarily an automorphism. ◻

We are now well on our way to describing generalized conjugacy structure for endomorphisms with kernels.

Lemma 2.6 *Any two elements in the same coset of* $\ker^\infty \phi$ *are* ϕ*-conjugate. That is,* ϕ*-conjugacy classes are unions of cosets of* $\ker^\infty \phi$*.*

Proof. Start with $x = y_0 z_0$, where $z_0 \in \ker^\infty \phi$. We wish to show that x and y_0 are ϕ-conjugate. Suppose, in particular, that $z_0 \in \ker^i \phi$. Define, iteratively,

$$\begin{aligned} y_{k+1} &= \phi(z_k)^{-1} x \\ z_{k+1} &= x^{-1} \phi(z_k) x \end{aligned}$$

Now, since $z_0 \in \ker^i \phi$, it follows that $x^{-1}\phi(z_0)x \in \ker^{i-1} \phi$, i.e. that $z_1 \in \ker^{i-1} \phi$. More generally, we can see inductively that

$$z_k \in \ker^{i-k} \phi.$$

It is immediate from the definitions of y_k and z_k that

$$x = y_k z_k$$

for all k. Combining this last equation with the definition of y_{k+1}, we obtain

$$y_{k+1} = \phi(z_k^{-1}) y_k z_k.$$

Thus, y_k is always ϕ-conjugate to y_{k+1}. By transitivity, y_n and y_m are ϕ-conjugate for any n, m. Now, take $k = i$. We have $z_i \in \ker^0 \phi$, so $z_i = 1$. Then $x = y_i$, so in fact x is ϕ-conjugate to all y_n. In particular, x is ϕ-conjugate to y_0. $\square$

The desired theorem follows easily.

Theorem 2.7 *There is a one-to-one correspondence between* ϕ*-conjugacy classes of* G *and* $\phi^{\ker}$*-conjugacy classes of* $G/\ker^\infty \phi$*; furthermore, each* ϕ*-conjugacy class is precisely* $|\ker^\infty \phi|$ *times as large as the corresponding* $\phi^{\ker}$*-cnjugacy class.*

Proof. We shall see that x and y are ϕ-conjugate if and only if the cosets $x \ker^\infty \phi$ and $y \ker^\infty \phi$ are $\phi^{\ker}$-conjugate. Suppose that $x = \phi(g) y g^{-1}$ holds for some g. Then the induced equation $x \ker^\infty \phi =$

$\phi^{\ker}(g\ker^\infty\phi)(y\ker^\infty\phi)(g^{-1}\ker^\infty\phi)$ follows. Conversely, if $x\ker^\infty\phi = \phi^{\ker}(g\ker^\infty\phi)(y\ker^\infty\phi)(g^{-1}\ker^\infty\phi)$ holds, then $xz = \phi(g)yg^{-1}$ holds for some $z \in \ker^\infty\phi$. xz is ϕ-conjugate to y, and we know by the preceding lemma that x is ϕ-conjugate to xz.

In general, then, a subset $\{x_1\ker^\infty\phi, \ldots, x_k\ker^\infty\phi\}$ is a $\phi^{\ker}$-conjugacy class if and only if the union $\bigcup_{i=1}^k x_i\ker^\infty\phi$ is a ϕ-conjugacy class. In addition, we note that the latter set is precisely $|\ker^\infty\phi|$ times as large as the former. $\square$

In light of this theorem, we may restrict our attention to generalized conjugacy classes produced by *auto*morphisms for the remainder of this paper. If we understood only the automorphism-produced generalized conjugacy classes for a group G and its quotients $G/\ker^\infty\phi$, then we could derive all generalized conjugacy class structures on G by the preceding theorem. But we would still first have to determine precisely what groups the quotients $G/\ker^\infty\phi$ are. Is it possible to predict what quotients of G we would have to look at, without spending interminable amounts of time computing iterated kernels?

Theorem 2.8 *A normal subgroup K of G is the iterated kernel of some endomorphism of G if and only if G is isomorphic to the semidirect product $G/K \ltimes K$.*

Proof. Recall that $G \simeq G/K \ltimes K$ is equivalent to the short exact sequence $K \xrightarrow{i} G \xrightarrow{p} G/K$ splitting. Let $s : G/K \to G$ denote such a splitting homomorphism. Suppose $K = \ker^\infty\phi$ for some endomorphism ϕ; we shall construct the splitting. Since we are dealing with finite groups only, it cannot be the case that $\ker^i\phi$ is a *proper* subgroup of $\ker^{i+1}\phi$ for all i: there is some integer M such that $\ker^i\phi = \ker^M\phi$ for all $i \geq M$, and hence $\ker^\infty\phi = \ker^M\phi$. Now, by construction, we have $\ker^i\phi = \ker\phi^i$, where ϕ^i is the i-fold composition of ϕ with itself. Thus $\ker^\infty\phi = \ker\phi^M$; it follows that $\operatorname{im}\phi^M \simeq G/\ker^\infty\phi$. The only element of $\ker^\infty\phi$ that lies in $\operatorname{im}\phi^M$ is 1: otherwise we contradict the assumption that $\ker^M\phi = \ker^\infty\phi$. Moreover, each coset of $\ker^\infty\phi$ contains at most one element of $\operatorname{im}\phi^M$: if $x, y \in \operatorname{im}\phi^M$ were in the same coset, then $x^{-1}y$ would be a nontrivial element of $\ker^\infty\phi$ that lies in $\operatorname{im}\phi^M$. But $|\operatorname{im}\phi^M|$ must equal $|G/\ker^\infty\phi|$, so each coset contains exactly one element of $\operatorname{im}\phi^M$. Define s by letting it take each coset to the unique member of $\operatorname{im}\phi^M$ contained in that coset. Then $p \circ s$ is the identity on $G/\ker^\infty\phi$.

Conversely, suppose that we have a splitting s. Let $\phi = s \circ p$. The only element of K lying in $\operatorname{im}\phi$ is 1;

it follows that $K = \ker^\infty \phi$. $\square$

Henceforth, only generalized conjugacy classes associated with automorphisms will be discussed.

2.2 Equivalence by Inner Automorphisms

In the examples listed in Section 1.2, three different generalized conjugacy class structures were given for A_5: one by the identity endomorphism, one by $\mathrm{Ad}_{(1\,5\,2)}$, and one by $\mathrm{Ad}_{(1\,2)}$. The first two of these are inner automorphisms, and the last is an outer automorphism. Moreover, the table shows that the two inner automorphisms produce combinatorially the same partition of the group into conjugacy classes. The conjugacy classes themselves are not the same (under $\mathrm{Ad}_{(1\,5\,2)}$, the identity element is generalized-conjugate to other elements of the group), but there is some bijection of G onto itself which carries *id*-conjugacy classes precisely onto $\mathrm{Ad}_{(1\,5\,2)}$-conjugacy classes. This observation is generalized in the following result:

Theorem 2.9 *Let $\phi_1, \phi_2 : G \to G$ be endomorphisms such that $\phi_1 = \mathrm{Ad}_p \circ \phi_2$ for some $p \in G$. Then there is a bijection $t : G \to G$ such that the image under t of each ϕ_1-conjugacy class is a ϕ_2-conjugacy class.*

Proof. Define $t : G \to G$ by $t(x) = px$. Now, suppose that $a, b \in G$ are ϕ_1-conjugate: $a = \phi_1(g)bg^{-1}$. Writing $a = p^{-1}t(a)$, $b = p^{-1}t(b)$, we compute:

$$\begin{aligned}
p^{-1}t(a) &= \phi_1(g)p^{-1}t(b)g^{-1} \\
t(a) &= p\phi_1(g)p^{-1}t(b)g^{-1} \\
t(a) &= \mathrm{Ad}_{p^{-1}}(\phi_1(g))t(b)g^{-1} \\
t(a) &= (\mathrm{Ad}_p^{-1} \circ \phi_1)(g)t(b)g^{-1} \\
t(a) &= \phi_2(g)t(b)g^{-1}
\end{aligned}$$

Thus, t carries ϕ_1-conjugate elements to ϕ_2-conjugate elements. The above computation can also be carried out in reverse to show that if t takes any two elements to image points that are ϕ_2-conjugate, then the original elements were ϕ_1-conjugate. That extablishes the desired property of t. $\square$

Thus, generalized conjugacy class structure is constant on cosets of $\operatorname{Inn} G$. In later sections we shall sometimes refer, say, to a ϕ_1-conjugacy class as being "the same as" a certain ϕ_2-conjugacy class, where of course we actually mean that the two classes under discussion are related by the bijection t given above.

2.3 Other Quick Lemmas

In an abelian group, all the ordinary conjugacy classes are the same size (namely, size 1). It turns out that all generalized conjugacy classes for fixed ϕ are the same size as well. We shall use additive notation.

PROPOSITION 2.10 *Given $\phi : G \to G$, where G is abelian, there are $|\ker(\phi - id)|$ ϕ-conjugacy classes, each of size $|\operatorname{im}(\phi - id)|$.*

Proof. $x, y \in G$ are ϕ-conjugate if and only if the following hold:

$$\begin{aligned} x &= \phi(g) + y - g \\ x - y &= \phi(g) - g \\ x - y &= (\phi - id)(g) \\ x - y &\in \operatorname{im}(\phi - id) \end{aligned}$$

The proposition follows. ◻

When G is a prime-power cyclic group, the preceding proposition is particularly easy to interpret.

COROLLARY 2.11 *Let $\phi : \mathbb{Z}_{p^r} \to \mathbb{Z}_{p^r}$ be the automorphism given by multiplication by k, where p does not divide k. Take p^s to be the largest power of p dividing $k-1$; if $k = 1$, take $p^s = p^r$. There are p^s ϕ-conjugacy classes each having size p^{r-s}.* ◻

The preceding corollary applies to the two examples involving $\mathbb{Z}_{27}$ given in Section 1.2.

For ordinary conjugation, we are assured that the identity falls into a conjugacy class by itself. That fact rarely holds for generalized conjugation, but for conjugation produced by an inner automorphism, we are at least guaranteed that *some* element falls into a conjugacy class by itself. But even that is quite a special property of inner automorphisms.

Proposition 2.12 *Let $\phi : G \to G$. There is ϕ-conjugacy class of size* 1 *if and only if ϕ is an inner automorphism.*

Proof. If ϕ is an inner automorphism, say Ad_x, then x^{-1} falls into a ϕ-conjugacy class by itself: for all g, we have

$$\phi(g)x^{-1}g^{-1} = (x^{-1}gx)x^{-1}g^{-1} = x^{-1}.$$

Conversely, suppose $x \in G$ is in a ϕ-conjugacy class by itself. For all g, $\phi(g)xg^{-1} = x$; we rewrite this equation as

$$\phi(g) = xgx^{-1}.$$

Thus $\phi = \mathrm{Ad}_{x^{-1}}$. $\square$

3 Maximal Generalized Conjugacy Classes

Let k_ϕ denote the number of ϕ-conjugacy classes in a group G. We wish to study the ratio $k_\phi/|G|$; in particular, we wish to find out when it is maximized. In the case that $\phi = id$, that ratio is maximized when G is abelian; indeed, that ratio is 1. It is known that for nonabelian groups, the ratio $k_{id}/|G|$ can be at most $\frac{5}{8}$. These facts about $k_{id}/|G|$ also apply to any $k_\phi/|G|$ whenever ϕ is an inner automorphism.

What happens when ϕ is an outer automorphism? We have already seen that ϕ-conjugacy classes are always of size at least 2 if ϕ is not inner, so $k_\phi/|G|$ is bounded above by $\frac{1}{2}$. Moreover, an infinite family of groups is known to achieve this bound.

Proposition 3.1 *Let A be an abelian group containing a direct summand of order* 4*. Then there is an automorphism ϕ of A such that $k_\phi/|A| = \frac{1}{2}$.*

Proof. A is of one of the two forms $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus B$ or $\mathbb{Z}_4 \oplus B$. On $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, the automorphism which exchanges the two direct summands produces two generalized conjugacy classes each of size 2; on $\mathbb{Z}_4$, the inversion automorphism does the same. Let ϕ be the direct sum of the identity automorphism on B with the appropriate preceding automorphism on the direct summand of order 4. To find the size of the ϕ-conjugacy classes, we compute the image of $\phi - id$: for $z \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$ or $\mathbb{Z}_4$, $b \in B$, we have

$$\begin{aligned}(\phi - id)(z + b) &= (\phi(z) + b) - (z + b) \\ &= \phi(z) - z.\end{aligned}$$

The image of $\phi - id$ is precisely the image of $\tau - id$, where τ denotes the previously considered automorphism on the direct summand of order 4. The τ-conjugacy classes were of size 2; hence, $|\operatorname{im}(\tau - id)| = 2$. It follows that every ϕ-conjugacy class is of size 2, so the number of ϕ-conjugacy classes is precisely half the order of the group. $\square$

Now, for ordinary conjugation, a group achieves $k_{id}/|G| = 1$ if and only if G is abelian. The question arises as to whether a similar result holds for generalized conjugation; that is, whether the groups in the family given above are the only ones having $k_\phi/|G| = \frac{1}{2}$ for some outer automorphism ϕ. The answer is not known in general; however, a partial result has been established.

Suppose we are given an outer automorphism $\phi : G \to G$ such that all ϕ-conjugacy classes are of size 2. Let α denote the non-identity element which is ϕ-conjugate to the identity. Note that Z_1^ϕ has index 2 in G. Also, we have

$$\phi(g) = \begin{cases} g & \text{if } g \in Z_1^\phi; \\ \alpha g & \text{if } g \notin Z_1^\phi. \end{cases}$$

Lemma 3.2 *Conjugates of α behave as follows:*

$$g^{-1}\alpha g = \begin{cases} \alpha & \textit{if } g \in Z_1^\phi; \\ \alpha^{-1} & \textit{if } g \notin Z_1^\phi. \end{cases}$$

Proof. First we consider the case $g \in Z_1^\phi$. Take any $h \notin Z_1^\phi$. Then we have $\phi(g) = g$ and $\phi(h) = \alpha h$, so $\phi(gh) = \phi(g)\phi(h) = g\alpha h$. But we also know that $gh \notin Z_1^\phi$, so $\phi(gh) = \alpha(gh)$. We equate $g\alpha h = \alpha g h$; it follows that $g^{-1}\alpha g = \alpha$.

Next, suppose $g \notin Z_1^\phi$. Again, pick $h \notin Z_1^\phi$. This time, $\phi(g)\phi(h) = \alpha g \alpha h$. But $gh \in Z_1^\phi$, so $\phi(gh) = gh$. We obtain $\alpha g \alpha h = gh$, which implies $g^{-1}\alpha g = \alpha^{-1}$. $\square$

PROPOSITION 3.3 *Suppose $\phi : G \to G$ produces generalized conjugacy classes all of size 2. Z_1^ϕ is a union of ϕ-conjugacy classes, as is its nontrivial coset.*

Proof. Note first that since ϕ fixes everything in Z_1^ϕ, and since Z_1^ϕ only has two cosets, $\phi(g)$ is always in the same coset of Z_1^ϕ as g itself. This means that for $g \notin Z_1^\phi$, we have $\alpha g \notin Z_1^\phi$. Those two membership relations imply that $\alpha \in Z_1^\phi$. Relying again on the fact that there are only two cosets, we find that all elements of the form yxy^{-1} or αyxy^{-1} must lie in the same coset of Z_1^ϕ that x lies in. But the ϕ-conjugate of x by y always looks like yxy^{-1} (for $y \in Z_1^\phi$) or αyxy^{-1} (for $y \notin Z_1^\phi$). Thus every ϕ-conjugacy class is contained in a single coset of Z_1^ϕ. □

COROLLARY 3.4 *If $\phi : G \to G$ produces generalized conjugacy classes all of size 2, then $|G|$ is divisible by 4.*

Proof. By the preceding proposition, Z_1^ϕ is a union of conjugacy classes, each of size 2, so $|Z_1^\phi|$ is even. And $|G| = 2|Z_1^\phi|$. □

Earlier, it was mentioned that for nonabelian groups, $k_\phi/|G|$ can be at most $\frac{5}{8}$.

CONJECTURE 3.5 *If ϕ is an outer automorphism, and if $k_\phi/|G| < \frac{1}{2}$, then $k_\phi/|G| \leq \frac{3}{8}$.*

Some justification for this conjecture will be given in the following sections.

4 Divisibility in Generalized Conjugacy Classes

4.1 Motivation

The goal of this and the remaining sections is to place some restrictions on the sizes of generalized conjugacy classes. A purely empirical observation that might be made on the basis of the examples given in Section 1.2 is that when ϕ is not an inner automorphism, ϕ-conjugacy classes tend to be larger in size and fewer in number than ordinary conjugacy classes. Can we say something more formal along those lines? For instance, can we place a lower bound on the GCD of the orders of the ϕ-conjugacy classes?

The work in the remaining sections will be motivated by the relatively easy solution to the question under certain special assumptions. In Section 1.2, one of the examples used the automorphism ϕ on D_{20}

given by $r \mapsto r^{13}$, $f \mapsto fr^{10}$. This gave arithmetically the same conjugacy class breakdown as did the other example with D_{20}, which used an endomorphism having a nontrivial kernel. More strikingly, however, this automorphism-produced generalized conjugacy class structure is "5 times" the ordinary conjugacy class structure on Z_1^ϕ, which happens to be isomorphic to D_4.

THEOREM 4.1 *Suppose that $C_1^\phi \cap Z_1^\phi = \{1\}$ and that Z_1^ϕ is a normal subgroup of G. Then there is a one-to-one correspondence between ϕ-conjugacy classes of G and ordinary conjugacy classes in Z_1^ϕ: each ϕ-conjugacy class is precisely $|C_1^\phi|$ times as large as the corresponding ordinary conjugacy class in Z_1^ϕ.*

Proof. Choose a transversal $\{g_1, \dots, g_k\}$ of Z_1^ϕ, where $k = |C_1^\phi|$. (Thus, $\{\phi(g_i)g_i^{-1}\}_{i=1}^k = C_1^\phi$.) Define a function $\omega : \{g_i\} \times Z_1^\phi \to G$ by $\omega(g_i, x) = \phi(g_i)xg_i^{-1}$. We list the values of ω in a table with the elements of Z_1^ϕ as the column headings:

$$\begin{array}{c|cccc}
 & 1 & \cdots & x & \cdots \\
\hline
1 & \phi(g_1)g_1^{-1} & & \phi(g_1)xg_1^{-1} & \\
\vdots & \vdots & \ddots & & \vdots \\
i & \phi(g_i)g_i^{-1} & & \omega(g_i, x) & \\
\vdots & \vdots & & & \ddots \\
k & \phi(g_k)g_k^{-1} & \cdots & \omega(g_k, x) & \cdots
\end{array}$$

Now, this table has precisely $k \cdot |Z_1^\phi| = |G|$ entries in it. We will show that every element of G is contained in the table; we will then describe ϕ-conjugacy in G in terms of this table. The domain of ω has the same size as G, so if we show that ω is injective, it would follow that every element of G occurs in the table. First we observe that if $g \notin Z_1^\phi$, then $\phi(g)$ is in a different coset of Z_1^ϕ than g is: if they were in the same coset, they would differ by an element of Z_1^ϕ, but in fact they differ by $\phi(g)g^{-1} \in C_1^\phi$, and C_1^ϕ has trivial intersection with Z_1^ϕ by assumption. ($\phi(g)g^{-1}$ lands in that intersection only if $g \in Z_1^\phi$.) Now, suppose that $\omega(g_m, x) = \omega(g_n, y)$. Rearranging the equation gives

$$x(g_m^{-1}g_n) = \phi(g_m^{-1}g_n)y. \tag{1}$$

This equation tells us that $g_m^{-1}g_n$ and $\phi(g_m^{-1}g_n)$ are contained in the same coset of Z_1^ϕ, so it follows that $g_m^{-1}g_n \in Z_1^\phi$. But since the set $\{g_i\}$ was chosen to be a transversal, $g_m^{-1}g_n$ can be in Z_1^ϕ only if $m = n$.

Plugging $g_m = g_n$ into Equation 1 gives $x = y$. Thus, ω is injective.

Now, when are $\omega(g_m, x)$ and $\omega(g_n, y)$ ϕ-conjugate? That is, when does there exist an h satisfying

$$\phi(g_m)xg_m^{-1} = \phi(h)\phi(g_n)yg_n^{-1}h^{-1}? \tag{2}$$

Certainly this is satisfied if $x = y$; we merely take $h = g_m g_n^{-1}$. It follows that each column of the above table is contained within a single ϕ-conjugacy class. On the other hand, if $x \neq y$, Equation 2 can be rewritten as

$$x\gamma = \phi(\gamma)y.$$

where $\gamma = g_m^{-1}hg_n$. As before, this implies that γ and $\phi(\gamma)$ lie in the same coset of Z_1^ϕ, and hence that $\gamma \in Z_1^\phi$ and $\phi(\gamma) = \gamma$. That last equation allows us to conclude that

$$y = \gamma^{-1}x\gamma$$

for some $\gamma \in Z_1^\phi$. That is, elements in different columns of the table give earlier can be ϕ-conjugate only if the members of Z_1^ϕ heading those columns are conjugate in the ordinary sense within Z_1^ϕ.

We conclude that ϕ-conjugacy classes in G are unions of columns of the table; two columns are in the same ϕ-conjugacy class if and only if their headings are in the same conjugacy class in Z_1^ϕ. $\square$

It is not to be hoped that a result of this sort holds in general; that is, the arithmetic of generalized conjugacy classes is not typically some multiple of the arithmetic of the ordinary conjugacy classes of some group. For instance, in Section 1.2, the structure induced on A_6 by $x \mapsto x^{(1\,2)}$ is

$$15 \times [1, 1, 6, 8, 8].$$

However, the expression in brackets is not the conjugacy class breakdown of *any* group of order 24! It cannot even be a generalized conjugacy class structure on some group of order 24, since the presence of classes of size 1 implies that it is produced by an inner automorphism.

4.2 Conjugation in the Action Group

In this section we shall actually describe generalized conjugation in terms of an ordinary conjugation action, but the latter shall occur in a larger group containing G as a normal subgroup, rather than in G itself or some subgroup thereof.

Definition 4.2 *Given an automorphism $\phi : G \to G$, we define*

$$\overline{\mathrm{Act}}_\phi\, G = \langle \phi \rangle \ltimes G,$$

called the **extended action group** *of ϕ on G. Suppose ϕ^i is the smallest power of ϕ which is an inner automorphism; in particular, suppose $\phi^i = \mathrm{Ad}_p$. Define*

$$\mathrm{Act}_\phi\, G = \overline{\mathrm{Act}}_\phi\, G / \langle \phi^i p^{-1} \rangle,$$

called the **action group** *of ϕ on G.*

Note that $\mathrm{Act}_\phi\, G$ is well defined because in $\overline{\mathrm{Act}}_\phi\, G$, we have $\phi^{-i} x \phi^i = p^{-1} x p$ for x, so $\langle \phi^i p^{-1} \rangle$ is in the center of $\overline{\mathrm{Act}}_\phi\, G$. Furthermore, since in constructing $\mathrm{Act}_\phi\, G$, we are taking the quotient by a subgroup having trivial intersection with G, G is still imbedded as a normal subgroup in $\mathrm{Act}_\phi\, G$.

Lemma 4.3 $\mathrm{Act}_\phi\, G \simeq \mathrm{Act}_{\phi \circ \mathrm{Ad}_p}\, G$ *for all $p \in G$.*

Proof. Consider the map $\mathrm{Act}_{\phi \circ \mathrm{Ad}_p}\, G \to \mathrm{Act}_\phi\, G$ which sends each element of G to itself and which sends the generator $\phi \circ \mathrm{Ad}_p$ to $p\phi$. This map clearly preserves the action of that generator on G; furthermore, it is well defined since powers of those generators which are inner automorphisms have been identified with the appropriate elements of G. $\square$

Now, recall that G is a normal subgroup of $\overline{\mathrm{Act}}_\phi\, G$. Thus, if we let G act on $\overline{\mathrm{Act}}_\phi\, G$ by conjugation, it respects the cosets of G. That is, $g^{-1} x g$ is always contained in the coset xG for any $g \in G$, $x \in \overline{\mathrm{Act}}_\phi\, G$. In particular, let us consider the action of G on the coset ϕG.

Proposition 4.4 *Given $x \in G$, the stabilizer of the element $\phi x \in \overline{\mathrm{Act}}_\phi\, G$ is precisely the subgroup Z_x^ϕ.*

Proof. Consider the following derivation, where $g \in G$:

$$\begin{aligned} g^{-1} \phi x g &= \phi x \\ \phi x &= g \phi x g^{-1} \\ x &= \phi^{-1} g \phi x g^{-1} \\ x &= \phi(g) x g^{-1} \end{aligned}$$

The first line of the previous is equivalent to the statement "g is in the stabilizer of ϕx under the conjugation action of G"; the last line is equivalent to "g is in the ϕ-centralizer of x." $\square$

Henceforth, the stabilizer of an element of $\overline{\mathrm{Act}}_\phi\, G$ under the conjugation action of G will be called simply the G-stabilizer of that element. Since the above correspondence between stabilizers and ϕ-centralizers holds, we have the following:

Corollary 4.5 *The orbits in ϕG under the conjugation action of G are in one-to-one correspondence with ϕ-conjugacy classes in G; each orbit is the same size as the corresponding ϕ-conjugacy class.* $\square$

The preceding two propositions do not directly give new combinatorial information about generalized conjugacy classes, but they offer a new framework in which to think about them. For yet another perspective, we note that the derivation in the proof of Proposition 4.4 is valid even if we take the quotient to eliminate powers of ϕ which are inner:

Proposition 4.6 *Proposition 4.4 and Corollary 4.5 hold if $\overline{\mathrm{Act}}_\phi\, G$ is replaced by $\mathrm{Act}_\phi\, G$.* $\square$

4.3 ϕ-Centralizer Containment

For ordinary conjugation in a group G, the following holds:

Fact 4.7 *Every centralizer is contained in a particular centralizer (namely that of the identity element).*

This fact and Lagrange's Theorem together imply that

Fact 4.8 *The order of a certain conjugacy class (namely that of the identity) divides the orders of all other conjugacy classes.*

Now, these are unquestionably somewhat trivial statements, since $Z_1^{id} = G$ and $|C_1^{id}| = 1$. At one time it was conjectured, however, that the above facts (with the parenthetical references to the identity deleted) held for generalized conjugacy classes. Indeed, to date the only known example violating them is that given in Section 1.2 as A_6 with automorphism τ.

Nevertheless, all the τ-conjugacy classes of A_6 have orders divisible by 18. It was hoped that a weaker reformulation of the above might hold:

STATEMENT 4.9 *Consider the smallest subgroup of G containing isomorphic copies of all ϕ-centralizers. The index of that subgroup is the GCD of the orders of the ϕ-conjugacy classes.*

However, this idea was invalidated when it was found that A_6 in fact contains no subgroup of index 18.

An important and enlightening result would be the discovery of some combinatorial property of automorphisms that would allow one to predict the GCD of the orders of ϕ-conjugacy classes without actually computing the members of the classes themselves. Ongoing work focuses on this goal.

4.4 Divisibility in Special Cases

We conclude with a result which achieves that goal under special assumptions, and only for some subset of the generalized conjugacy classes produced by a given automorphism. Throughout this section, ϕ and ψ denote automorphisms with the property that $\phi\psi^{-1}$ is an inner automorphism. The notation $\operatorname{Act} G$ will be used to denote the isomorphic groups $\operatorname{Act}_\phi G$ and $\operatorname{Act}_\psi G$.

Now, any element which G-stabilizes ψ also G-stabilizes ψ^n. Futhermore, two automorphisms in the same orbit of G's action on $\operatorname{Act} G$ clearly have isomorphic G-stabilizers. These observations lead us to the following lemma.

LEMMA 4.10 *Suppose that for some n, ψ^n is in the same G-orbit as ϕ. Then the G-stabilizer of ϕ contains an isomorphic copy of the G-stabilizer of ψ.* $\square$

Next, we know for general group actions that the stabilizer of a given element is contained in the stabilizer of any power of that element. But that fact is relevant for our discussion only when a power of an element in ϕG also lies in ϕG. The following lemma describes one case where that fact applies. Note that the order of $\operatorname{Act} G$ divides the orders of $\overline{\operatorname{Act}}_\phi G$ and $\overline{\operatorname{Act}}_\psi G$.

LEMMA 4.11 *If $|\overline{\operatorname{Act}}_\psi G|/|\operatorname{Act} G|$ is relatively prime to $|\operatorname{Act} G|/|G|$, then there is some power of ψ, say ψ^i, such that ψ^{i-1} is inner and such that $|\overline{\operatorname{Act}}_{\psi^i} G|/|\operatorname{Act} G| = 1$.*

Proof. Let us write $n = |\overline{\operatorname{Act}}_\psi G|/|\operatorname{Act} G|$, $m = |\operatorname{Act} G|/|G|$. Note that $mn = |\overline{\operatorname{Act}}_\psi G|/|G| = |\langle\psi\rangle|$; additionally, m is the smallest power of ψ which is inner. Now, consider the quotient $\operatorname{Act} G/G$: this is a cyclic group of order m; and since n is relatively prime to m, the coset containing ψ^n is a generator for that cyclic group. In particular, some power of ψ^n, say ψ^{nk}, is contained in the coset containing ψ itself. Take $i = nk$. Now $\psi^i\psi^{-1}$ must be contained in the identity coset, i.e. in G itself, so ψ^{i-1} is inner. Additionally, ψ^i has order at most m (which is the order of ψ^n). Since the coset containing ψ^i generates $\operatorname{Act} G$, it follows that ψ^i is a generator for $\langle\psi^n\rangle$, so ψ^i has order m. Therefore, $|\overline{\operatorname{Act}}_{\psi^i} G|/|\operatorname{Act} G| = 1$. $\square$

Corollary 4.12 *If $|\overline{\operatorname{Act}}_{\psi} G|/|\operatorname{Act} G|$ is relatively prime to $|\operatorname{Act} G|/|G|$, and i is as above, then the order of the G-stabilizer of ψ divides the order of the G-stabilizer of ψ^i.* $\square$

The above lemmas are straightforward and elementary, but they illustrate the utility of the $\operatorname{Act} G$ construction. In Section 1.1, when we defined ϕ-conjugation, we were dealing with a group acting on a set. Now we have transformed the question into one of a group, G, acting on another group, $\operatorname{Act} G$. The permutations on $\operatorname{Act} G$ associated to given elements of G are in fact autmorphisms of $\operatorname{Act} G$. The resultant extra algebraic structure facilitates proving lemmas such as the preceding which do not even have easily-stated analogues in the language of ϕ-conjugation alone. For instance, Lemma 4.10 might be restated as follows:

Proposition 4.13 *Let $x, y \in G$; let $\tilde{x}, \tilde{y}$ be corresponding elements in $\phi G \subseteq \operatorname{Act}_\phi G$. If for some n, $\tilde{y}^n$ is in the same G-orbit as $\tilde{x}$, then $|Z_y^\phi|$ divides $|Z_x^\phi|$. Equivalently, $|C_x^\phi|$ divides $|C_y^\phi|$.* $\square$

This proposition is both powerful and widely applicable. It is hoped that similarly strong statements about generalized conjugacy classes may be proven with the aid of the action group construction.

References

[1] O. Davey, E. Hart, and K. Trapp, Computation of Nielsen numbers for maps of closed surfaces, *Transactions of the AMS* **14**, 115-117 (1992).

[2] D.W. Miller, On a Theorem of Hölder, *Amer. Math. Monthly* **65**, 252–254 (1958).