Orbits of Irreducible Representations of D_n Modulo $Aut(D_n)$

Yuguang (Roger) Bai, 998141577

December 5, 2017

Let G be a finite group and V a finite dimensional vector space over $\mathbb{C}$. Then if $\rho : G \to GL(V)$ is a representation of G and $\alpha \in Aut(G)$, we have $\rho \circ \alpha$ to be another representation of G. We see that ρ is irreducible if and only if $\rho \circ \alpha$ is irreducible, as $\rho(G) \cdot W \subseteq W$ if and only if $\rho \circ \alpha(G) \cdot W = \rho(G) \cdot W \subseteq W$ for a subspace $W \subseteq V$. Thus $Aut(G)$ acts on the irreducible representations of G via composition. We are interested in finding the orbits of this action when $G = D_n$, the dihedral group of order $2n$.

We will view $D_n = \langle r, s : r^n = s^2 = 1, srs = r^{-1} \rangle = \{r^m : 0 \leq m \leq n-1\} \sqcup \{r^\ell s : 0 \leq \ell \leq n-1\}$ where the elements r^m will be called rotations and the elements $r^\ell s$ will be called reflections. To start understanding the action of $Aut(D_n)$, we first describe $Aut(D_n)$ itself. As every automorphism of D_n is determined by where it sends the generators r and s, we will denote ${}_x\alpha_y : D_n \to D_n$ to be the homomorphism that sends $r \mapsto x$ and $s \mapsto y$.

Proposition 1. *$Aut(D_2) \cong S_3$ and for $n \geq 3$, $Aut(D_n) = \{{}_{r^k}\alpha_{r^j s} : 0 \leq k, j \leq n-1, \gcd(k,n) = 1\}$.*

Proof. We have $D_2 \cong V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the Klein 4-group. Every automorphism of D_2 fixes the identity and permutes the other three elements. Thus we can view $Aut(D_2)$ as a subgroup of S_3. It is a simple calculation to show that every permutation of the nontrivial elements gives an automorphism, hence $Aut(D_2) \cong S_3$.

Now let $n \geq 3$ and let $\alpha \in Aut(D_n)$. As r has order n, we have the order of $\alpha(r)$ to also be n. The only elements of order $n \geq 3$ in D_n are r^k where $\gcd(k,n) = 1$, so $\alpha(r) = r^k$ for such a k. As $\gcd(k,n) = 1$, r^k is a generator for $\langle r \rangle$ and so $\alpha(\langle r \rangle) = \langle r \rangle$. As s has order 2, $\alpha(s)$ also has order 2. The only elements of order 2 in D_n are $r^j s$ for some $0 \leq j \leq n-1$ and $r^{n/2}$ if n is even. However, we showed $\alpha(\langle r \rangle) = \langle r \rangle$. As α is injective, we cannot have $\alpha(s)$ to be in $\langle r \rangle$, and so $\alpha(s) = r^j s$ for some $0 \leq j \leq n-1$. Thus $\alpha =_{r^k} \alpha_{r^j s}$. Conversely, to show $\alpha \coloneqq {}_{r^k}\alpha_{r^j s}$, $\gcd(k,n) = 1$, is an automorphism, it suffices to show it is surjective as D_n is finite. Using the same argument as above, as $\gcd(k,n) = 1$, we have $\langle r \rangle \subseteq \alpha(D_n)$. Let $r^\ell s \in D_n$. Let $x \in D_n$ such that $\alpha(x) = r^{\ell - j}$. Then

$$\alpha(xs) = \alpha(x)\alpha(s) = r^{\ell-j} r^j s = r^\ell s$$

so $r^\ell s \in \alpha(D_n)$. Thus $\alpha(D_n)$ contains all rotations and reflections so α is surjective, and hence an automorphism. $\square$

We now look at the irreducible representations of D_n and see how $Aut(D_n)$ acts on them. As every irreducible representation is uniquely determined by its character, $Aut(D_n)$ acts on the character table of D_n, and this will allow us to determine the orbits of the action. Chapter 5 of [1] provides us with the irreducible representations and characters of D_n.

We first consider the case when $n \geq 3$ is odd. There are two 1-dimensional representations: the trivial representation tr which sends every element to 1, and representation det which sends rotations to 1 and reflections to -1. Let $\omega = e^{\frac{2\pi i}{n}}$. The $\frac{n-1}{2}$ irreducible 2-dimensional representations are

$$\begin{aligned} \rho_\ell : \ r &\mapsto \begin{bmatrix} \omega^\ell & 0 \\ 0 & \omega^{-\ell} \end{bmatrix} \\ s &\mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{aligned}$$

where $1 \leq \ell \leq \frac{n-1}{2}$. The character table for D_n in this case is the following, where $[x]$ denotes the conjugacy class of x:

	$[1]$	$[s]$	$[r^m]$,$1 \leq m \leq \frac{n-1}{2}$
tr	1	1	1
det	1	-1	1
ρ_ℓ	2	0	$2\cos(\frac{2\pi \ell m}{n})$

It is clear that the trivial representation tr is fixed by every automorphism so it is its own orbit. Since automorphisms fix the identity, the dimension of each representation is invariant under the action of $Aut(D_n)$, and so det, the only other 1-dimensional representation, is also fixed by every automorphism. Now let $\alpha := {}_{r^k}\alpha_{r^j s} \in Aut(D_n)$. Then

$$\operatorname{trace}(\rho_\ell \circ \alpha(r^m)) = \operatorname{trace}(\rho_\ell(r^{km})) = 2\cos\left(\frac{2\pi \ell k m}{n}\right).$$

Thus comparing characters, we have $\rho_\ell \circ \alpha \simeq \rho_{k\ell \mod n}$. Then given a 2-dimensional representation ρ_ℓ, its orbit consists of 2-dimensional representations ρ_a where $a \equiv \ell k \mod n$ for some k with $\gcd(k, n) = 1$. Thus we are really considering the orbits of $(\mathbb{Z}/n\mathbb{Z})\backslash\{0\}$ under the action of $(\mathbb{Z}/n\mathbb{Z})^* \cong Aut(\mathbb{Z}/n\mathbb{Z})$, the group of units of $\mathbb{Z}/n\mathbb{Z}$. We shall proceed with finding the orbits of this new action in order to answer the original question.

Proposition 2. *Let $a, b \in \mathbb{Z}/n\mathbb{Z}$ and suppose there exists $u \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $a \equiv bu \mod n$. Then $\gcd(a, n) = \gcd(b, n)$.*

Proof. Suppose d divides b and n. Then since $a \equiv bu \mod n$, we have $cn = a - bu$ for some c. Then d divides $cn + bu = a$. Thus $\gcd(b, n)$ divides $\gcd(a, n)$. Now suppose d divides a and n. Then as $cn = a - bu$ for some c, d divides bu. Since $\gcd(u, n) = 1$ and d divides n, we have d divides b. Thus $\gcd(a, n)$ divides $\gcd(b, n)$, so they must be equal. □

Proposition 2 allows us to conclude that every orbit is contained in $\{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = d\}$ for some divisor d of n. In fact, these sets are all the orbits.

Proposition 3. *Let $a \in \mathbb{Z}/n\mathbb{Z}$ be such that* $\gcd(a, n) = d$*. Then there exists $u \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $au \equiv d \mod n$.*

Proof. First consider the case when $n = p^t$ for some prime p. Let k be such that $kd = n$. Consider the cyclic subgroup $d(\mathbb{Z}/k\mathbb{Z}) = \{0, d, 2d, ..., (k-1)d\} \leq \mathbb{Z}/n\mathbb{Z}$. As subgroups of cyclic groups are uniquely characterized by their size and $\langle a \rangle$ has size $\frac{n}{d} = k$, we have $a \in d(\mathbb{Z}/k\mathbb{Z})$. Suppose $a = md$ for some m. As $a = md$ is a generator of $d(\mathbb{Z}/k\mathbb{Z})$, then $\gcd(m, k) = 1$ so there exists $u \in (\mathbb{Z}/k\mathbb{Z})^*$ such that $mu \equiv 1 \mod k$. View u as an element of $\mathbb{Z}/n\mathbb{Z}$ coprime to k. Since k divides $1 - mu$, then $n = kd$ divides $d(1 - mu) = d - dmu$ so $au = dmu \equiv d \mod n$. As $n = p^t$, then k is also a power of the prime p. Since $\gcd(u, k) = 1$, we have $\gcd(u, n) = 1$ so $u \in (\mathbb{Z}/n\mathbb{Z})^*$.

For the general case, suppose $n = p_1^{t_1} \cdots p_\ell^{t_\ell}$ is a product of distinct primes. By the Chinese Remainder Theorem, we have a ring isomorphism $\phi : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \prod_{i=1}^{\ell} \mathbb{Z}/p_i^{t_i}\mathbb{Z}$. I claim that this isomorphism restricts to an isomorphism

$$\begin{array}{rcl} \phi_* : (\mathbb{Z}/n\mathbb{Z})^* & \xrightarrow{\sim} & \prod_{i=1}^{\ell} (\mathbb{Z}/p_i^{t_i}\mathbb{Z})^* \\ u & \mapsto & (u \mod p_i^{t_i})_{i=1}^{\ell} \end{array}$$

Indeed, if u is coprime to $n = p_1^{t_1} \cdots p_\ell^{t_\ell}$, then u is coprime to $p_i^{t_i}$ for each i, so ϕ_* is well-defined. As ϕ is injective, so is $\phi_* = \phi|_{(\mathbb{Z}/n\mathbb{Z})^*}$. Let φ be the Euler Totient function, that is, $\varphi(n) = \#\{k \in \{1, ..., n-1\} : \gcd(k, n) = 1\}$. Then $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$ and

$$\begin{aligned} \left| \prod_{i=1}^{s} (\mathbb{Z}/p_i^{t_i}\mathbb{Z})^* \right| &= \prod_{i=1}^{s} \varphi(p_i^{t_i}) \\ &= \prod_{i=1}^{s} p_i^{t_i}(1 - \frac{1}{p_i}) \\ &= n \prod_{\substack{p \mid n \\ p \text{ prime}}} (1 - \frac{1}{p}) \\ &= \varphi(n) \end{aligned}$$

As ϕ_* is injective between two finite sets of the same size, it is therefore an isomorphism.

As $\gcd(a, n) = d$, then a has order $\frac{n}{d}$, which is the same as d. I claim that this implies $a \mod {}_{p_i^{t_i}}$ has the same order as $d \mod {}_{p_i^{t_i}}$ for all i, that is, $\gcd(a, p_i^{t_i}) = \gcd(d, p_i^{t_i})$ for all i. Indeed, if δ divides a and $p_i^{t_i}$, then δ divides n as $p_i^{t_i}$ divides n. Then δ divides $\gcd(a, n) = d$ so δ divides $\gcd(d, p_i^{t_i})$. If δ divides d and $p_i^{t_i}$, then δ divides $\gcd(a, n) = d$ so δ divides a. Thus $\gcd(a, p_i^{t_i}) = \gcd(d, p_i^{t_i})$. By the special case above, there exists $u_i \in (\mathbb{Z}/p_i\mathbb{Z})^*$ such that $au_i \equiv d \mod p_i^{t_i}$. By the isomorphism ϕ_*, there exists $u \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $\phi_*(u) = (u_i \mod p_i^{t_i})$. Then

$$\phi(au) = (a \mod p_i^{t_i})(u_i \mod p_i^{t_i}) = (d \mod p_i^{t_i}) = \phi(d)$$

so $au \equiv d \mod n$. $\square$

Thus the orbits of $(\mathbb{Z}/n\mathbb{Z})\backslash\{0\}$ modulo the action of $Aut(\mathbb{Z}/n\mathbb{Z})$ are $\{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = d\}$ for every divisor d of n. Combining the above results, we get the following:

Theorem 4. *For n odd, the orbits of irreducible 2-dimensional representations of D_n modulo the action of $Aut(D_n)$ are $\{tr\}$, $\{det\}$, and $\{\rho_\ell : \gcd(\ell, n) = d\}$ for every divisor $d \neq n$ of n.*

Remark 5. It is a basic result of number theory that $\{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = d\}$ has size $\varphi(\frac{n}{d})$ where φ is the Euler Totient function. Thus the orbit $\{\rho_\ell : \gcd(\ell, n) = d\}$ has size $\frac{1}{2}\varphi(\frac{n}{d})$ as $1 \leq \ell \leq \frac{n-1}{2}$.

Corollary 6. *The irreducible faithful 2-dimensional representations of D_n are ρ_u where* $\gcd(u, n) = 1$.

Proof. Note that if ρ is a representation of a group G and $\alpha \in Aut(G)$, then ρ is a faithful representation if and only if $\rho \circ \alpha$ is a faithful representation, as automorphisms α and α^{-1} are injective. Consider ρ_d with $d > 1$ a divisor of n, say $kd = n$. Then

$$\rho_d(r^k) = \begin{bmatrix} \omega^{kd} & 0 \\ 0 & \omega^{kd} \end{bmatrix} = I = \rho_d(1)$$

so ρ_d is not faithful. A simple calculation shows that ρ_1 is a faithful representation so all faithful 2-dimensional representations of D_n are in the orbit of ρ_1, that is, $\{\rho_u : \gcd(u, n) = 1\}$. $\square$

Now consider the case when n is even. There are four 1-dimensional representations: the trivial representation tr which sends all elements to 1, det which sends rotations to 1 and reflections to -1, δ which sends $r \mapsto -1$ and $s \mapsto 1$, and τ which sends $r \mapsto -1$ and $s \mapsto -1$. We also have $\frac{n-2}{2}$ irreducible 2-dimensional representations, denoted

$$\begin{aligned} \rho_\ell : \quad r &\mapsto \begin{bmatrix} \omega^\ell & 0 \\ 0 & \omega^{-\ell} \end{bmatrix} \\ s &\mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{aligned}$$

for $1 \leq \ell \leq \frac{n-2}{2}$. The character table for D_n is:

	$[1]$	$[s]$	$[rs]$	$[r^m], 1 \leq m \leq \frac{n}{2}$
tr	1	1	1	1
det	1	-1	-1	1
δ	1	1	-1	$(-1)^m$
τ	1	-1	1	$(-1)^m$
ρ_ℓ	2	0	0	$2\cos\left(\frac{2\pi\ell m}{n}\right)$

We first deal with the case when $n = 2$. In this case, there are no 2-dimensional representations. The trivial representation is fixed by every automorphism so it is its own orbit. Let $\alpha \in Aut(D_2)$ be the automorphism that sends $r \mapsto s \mapsto rs \mapsto r$. Then we have a new table of characters:

	$[s]$	$[rs]$	$[r]$	
$det \circ \alpha$	-1	1	-1	$= \tau$
$\delta \circ \alpha$	-1	-1	1	$= det$
$\tau \circ \alpha$	1	-1	-1	$= \delta$

so the nontrivial 1-dimensional representations form their own orbit.

Now consider the case when $n > 2$ and is even. Again, the trivial representation is fixed by all automorphisms. Let $\alpha :=_{r^k} \alpha_{r^j s} \in Aut(D_n)$. Then we have a new table of characters:

	$[s]$	$[rs]$	$[r^m]$
$det \circ \alpha$	-1	-1	1
$\delta \circ \alpha$	$(-1)^j$	$(-1)^{k+j}$	$(-1)^{km}$
$\tau \circ \alpha$	$(-1)^{j+1}$	$(-1)^{k+j+1}$	$(-1)^{km}$
$\rho_\ell \circ \alpha$	0	0	$2\cos\left(\frac{2\pi\ell km}{n}\right)$

Thus det is fixed by all automorphisms while δ and τ are in the same orbit. We also see that $\rho_\ell \circ \alpha \simeq \rho_{k\ell \mod n}$. Note that in the arguments for determining the orbits of the 2-dimensional representations when n was odd, no where did we use the fact that n was odd. Hence using the same arguments as above, we get the following:

Theorem 7. *For n even, the orbits of the irreducible representations of D_n modulo the action of $Aut(D_n)$ are*

$$\begin{array}{cl} \{tr\} \text{ and } \{det, \delta\tau\} & for\ n = 2 \\ \{tr\}, \{det\}, \{\delta, \tau\}, \text{ and } \{\rho_\ell : \gcd(\ell, n) = d\}_{d|n, d \notin \{\frac{n}{2}, n\}} & for\ n \geq 2 \end{array}$$

Note that in the above theorem, $d \neq \frac{n}{2}$ as $\rho_{n/2}$ is not irreducible and that $\frac{n}{2}$ is fixed by all units of $\mathbb{Z}/n\mathbb{Z}$ due to Proposition 2. As before, the irreducible 2-dimensional faithful representations consists of the orbit $[\rho_1]$.

References

[1] Serre, J.-P., *Linear Representations of Finite Groups*, Springer-Verlag, New York, 1977.

[2] Sommer-Simpson, J. (2013, November 2). *Automorphism Groups for Semidirect Products of Cyclic Groups.* Retrieved from http://math.uchicago.edu/~may/REU2013/REUPapers/Sommer-Simpson.pdf