On Commutation Semigroups of Dihedral Groups

Darien DeWolf, Charles Edmunds, Christopher Levy

October 13, 2012

Some Definitions to Start

Definition

For any group G with $g \in G$, the right and left commutation mappings associated with g are the mappings $\rho(g)$ and $\lambda(g)$ from G to G defined as

$$(x)\rho(g) = [x, g]$$

$$(x)\lambda(g) = [g, x],$$

where the commutator of g and h is defined as $[g, h] = g^{-1}h^{-1}gh$.

Definition

The set $\mathcal{M}(G)$ of all mappings from G to G forms a semigroup under composition of mappings.

Definition

The *right commutation semigroup of* G, $\mathrm{P}(G)$, is the subsemigroup of $\mathcal{M}(G)$ generated by the set of ρ-*maps* and *the left commutation semigroup of* G, $\Lambda(G)$, is the subsemigroup of $\mathcal{M}(G)$ generated by the set of λ-*maps*.

Definition

The dihedral group of order $2m$ has presentation

$$D_m = \left\langle a, b; a^m = 1, b^2 = 1, a^b = a^{-1} \right\rangle,$$

where the conjugate of a by b is denoted $a^b = b^{-1}ab$.

An Anomaly Presents Itself

Though $\mathrm{P}(G)$ and $\Lambda(G)$ have apparently symmetric definitions, it is not true in general that $\mathrm{P}(G) = \Lambda(G)$. In fact it is not even true in general that $\mathrm{P}(G) \cong \Lambda(G)$, for $|\mathrm{P}(D_3)| = 6 \neq 9 = |\Lambda(D_3)|$.
We then ask ourselves: "What conditions on the group can impose to force its commutation semigroups to be of equal order, isomorphic, equal?" We will focus now on dihedral groups.

Some Preliminaries

Notation

For each $s \geq 0$ let $\alpha_s = (-1)^s$ and $\beta_s = (-1)^s - 1$. Since the values of α_s and β_s are unique up to parity, it will cause no ambiguity to view s as an element of $\mathbb{Z}_2$.

Lemma

Let D_m be the dihedral group with presentation as above. For each $i, r \in \mathbb{Z}_m$ and $j, s \in \mathbb{Z}_2$:

$$(a^i b^j)\rho(a^r b^s) = a^{N_\rho} \text{ and } (a^i b^j)\lambda(a^r b^s) = a^{N_\lambda},$$

where $N_\rho \equiv i\alpha_j\beta_s - r\alpha_s\beta_j \equiv (-2)\alpha_{js}(is - jr) (\mathrm{mod}\, m)$ and $N_\lambda \equiv -N_\rho \equiv 2\alpha_{js}(is - jr) (\mathrm{mod}\, m)$.

Definition

For each pair $(A, B) \in \mathbb{Z}_m \times \mathbb{Z}_m$ we define a μ-map $\mu(A, B) : D_m \to D_m$ by

$$(a^i b^j)\mu(A, B) = a^{N_\mu}, \text{ where } N_\mu = Ai\alpha_j - B\beta_j.$$

Lemma

For each $r \in \mathbb{Z}_m$ and $s \in \mathbb{Z}_2$,

(i) $\rho(a^r b^s) = \mu(\beta_s,\ r\alpha_s)$,

(ii) $\lambda(a^r b^s) = \mu(-\beta_s, -r\alpha_s)$.

Lemma

For each $A, A' \in \mathbb{Z}_m$ and $B, B' \in \mathbb{Z}_2$,
$\mu(A, B) \circ \mu(A', B') = \mu(AA', BA')$.

Containers of μ-maps

Definition

If $A, B \in \mathbb{Z}_m$, the (A, B)-*container* is defined as

$$\mathcal{C}(A, B) = \{\mu(A, xB) : x \in \mathbb{Z}_m\}.$$

Lemma

For all $A, A', B, B' \in \mathbb{Z}_m$, $\mathcal{C}(A, B) \cap \mathcal{C}(A', B') \neq \varnothing$ if and only if $A \equiv A' (\mathrm{mod}\, m)$.

Lemma

$\mathrm{P}(D_n) \supseteq \{\rho_g\} = \mathcal{C}(0, 1) \dot{\cup} \mathcal{C}(-2, 1)$ *and*
$\Lambda(D_n) \supseteq \{\lambda_g\} = \mathcal{C}(0, 1) \dot{\cup} \mathcal{C}(2, 1)$.

Definition

For any two containers $\mathcal{C}(A, B)$ and $\mathcal{C}(A', B')$, we define their product as:

$$\mathcal{C}(A, B) \circ \mathcal{C}(A', B') = \left\{ \mu_1 \circ \mu_2 : \mu_1 \in \mathcal{C}(A, B), \mu_2 \in \mathcal{C}(A', B') \right\}.$$

Lemma

For $A, A' \in \mathbb{Z}_m$ and $B, B' \in \mathbb{Z}_2$, $\mathcal{C}(A, B) \circ \mathcal{C}(A', B') = \mathcal{C}(AA', BA')$.

Lemma

For $A, B \in \mathbb{Z}_m$,

(i) $\mathcal{C}(0, 1) \circ \mathcal{C}(A, B) \subseteq \mathcal{C}(0, 1)$,

(ii) $\mathcal{C}(A, B) \circ \mathcal{C}(0, 1) \subseteq \mathcal{C}(0, 1)$.

Definition

For $x \in \mathbb{Z}$, let $ind_m(x)$ be the smallest positive integer such that there is a $per_m(x) \in \mathbb{Z}^+$ with $x^{ind_m(x)} = x^{ind_m(x)+per_m(x)}$ and $per_m(x)$ the least such positive integer. Here $ind_m(x)$ and $per_m(x)$ are called the *index* and the *period* of x,

Lemma

If $m = 2^\ell n \geq 3$ *with* n *odd,* $\ell \geq 0$, *and* $n \geq 1$, *then for* $x \in \{-2, 2\}$

(i) *if* m *is odd, then* $ind_m(x) = 1$ *and* $per_m(x) = ord_m(x)$,

(ii) *if* m *is even and* $n > 1$, *then* $ind_m(x) = \ell$,

(iii) *if* m *is even and* $n = 1$, *then* $ind_m(x) = \ell$ *and* $per_m(x) = 1$.

Theorem

For $m = 2^\ell n \geq 3$ with n odd, $\ell \geq 0$, and $n \geq 1$,

$$\mathrm{P}(D_m) = \mathcal{C}(0,1) \cup \left(\bigcup_{i=1}^{t} \mathcal{C}((-2)^i, (-2)^{i-1}) \right),$$

(i)

$$\text{where } t = \begin{cases} ord_m(-2) \text{ for } \ell = 0,\ n > 1 \\ \ell + per_m(-2) - 1 \text{ for } \ell > 0,\ n > 1 \\ \ell - 1 \text{ for } \ell > 0,\ n = 1 \end{cases}$$

$$\Lambda(D_m) = \mathcal{C}(0,1) \cup \left(\bigcup_{i=1}^{t'} \mathcal{C}(2^i, 2^{i-1}) \right),$$

(ii)

$$\text{where } t' = \begin{cases} ord_m(2) \text{ for } \ell = 0,\ n > 1 \\ \ell + per_m(2) - 1 \text{ for } \ell > 0,\ n > 1 \\ \ell - 1 \text{ for } \ell > 0,\ n = 1 \end{cases},$$

and these unions are disjoint.

Definition

The *upper central series of a group* G is the series of subgroups of G,

$$Z_0(G) \leq Z_1(G) \leq \cdots \leq Z_n(G) \leq \cdots$$

with $Z_0(G) = \{1\}$ and $Z_n(G) =$
$\{g \in G : [g, g_1, g_2, \ldots, g_n] = 1, \text{ for all } g_1, g_2, \ldots, g_n \in G\}$. We call $Z_n(G)$ the n-th-centre of G and, where no ambiguity arises, denote it Z_n.

Theorem

(a) *If $u \geq 0$ and m is odd, then $Z_u(D_m) = \{1\}$,*

(b) *If $u \geq 0$ and m is even with $m = 2^\ell n$ ($n > 0$ and n odd), then*

(i) *if $n > 1$, then*

$$Z_u(D_m) = \begin{cases} \left\{a^N : N = (2^{\ell-u}n)x \text{ and } 0 \leq x < 2^u\right\}, u < \ell \\ \left\{a^{nx} : 0 \leq x < 2^\ell\right\}, u \geq \ell \end{cases}$$

(ii) *if $n = 1$, then*

$$Z_u(D_m) = \begin{cases} \left\{a^N : N = 2^{\ell-u}x \text{ and } 0 \leq x < 2^u\right\}, u < \ell \\ D_m, u \geq \ell \end{cases}$$

Theorem

If $u > 0$ and $Z_u(D_m) \leq \langle a \rangle$, then

(i) $\left|\mathcal{C}((-2)^u, (-2)^{u-1})\right| = \dfrac{m}{|Z_u(D_m)|}$,

(ii) $\left|\mathcal{C}(2^u, 2^{u-1})\right| = \dfrac{m}{|Z_u(D_m)|}$.

Lemma

$|\mathcal{C}(0, 1)| = \dfrac{m}{|Z_1|}$.

The Main Theorem

Theorem

If $m = 2^{\ell} n > 3$ *with* n *odd,*

$$|\mathrm{P}(D_m)| = m\left(\frac{1}{|Z_1|} + \sum_{i=1}^{t-1} \frac{1}{|Z_i|}\right)$$

(i)

$$\text{where } t = \begin{cases} 1 + ord_m(-2) \text{ for } \ell = 0,\ n > 1 \\ \ell + per_m(-2) \text{ for } \ell > 0,\ n > 1 \\ \ell \text{ for } \ell > 0,\ n = 1 \end{cases}$$

$$|\Lambda(D_m)| = m\left(\frac{1}{|Z_1|} + \sum_{i=1}^{t'-1} \frac{1}{|Z_i|}\right)$$

(ii)

$$\text{where } t' = \begin{cases} 1 + ord_m(2) \text{ for } \ell = 0,\ n > 1 \\ \ell + per_m(2) \text{ for } \ell > 0,\ n > 1 \\ \ell \text{ for } \ell > 0,\ n = 1 \end{cases}$$