Math 521A

7.2 – Basic Properties of Groups

To make the notation a little less cumbersome, we will replace the group operation $*$ with juxtaposition. So, instead of writing $a * b$, we will simply write ab.

Theorem

Let G be a group. Then:

1. *The identity element is unique.*
2. *Each element of G has a unique inverse.*
3. *Cancellation holds in G: $ab = ac \Rightarrow b = c$ for all $a, b, c \in G$.*

N.B.: $ab = ca$ does not imply that $b = c$ unless G is Abelian.

Theorem

Let G be a group, and $a, b \in G$. Then:

1. $(ab)^{-1} = b^{-1}a^{-1}$.
2. $(a^{-1})^{-1} = a$.

- Let k be a positive integer, G a group with identity e, and $a \in G$. We define $a^0 = e$ and

$$a^k = \underbrace{a \cdot a \cdots a \cdot a}_{k \text{ copies}} \quad \text{or} \quad ka = \underbrace{a + a + \cdots + a}_{k \text{ copies}}.$$

  Also,

$$a^{-k} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1} \cdot a^{-1}}_{k \text{ copies}} \quad \text{or} \quad (-k)a = \underbrace{(-a) + \cdots + (-a)}_{k \text{ copies}}.$$

- It follows that:

$$\begin{cases} a^{m+n} = a^m \cdot a^n \\ (a^m)^n = a^{mn} \end{cases} \quad \text{or} \quad \begin{cases} (m+n)a = ma + na \\ m(na) = (mn)a \end{cases}$$

  for all $m, n \in \mathbb{Z}$.

Order of an element: Let G be a group and $a \in G$. The order of a, denoted as $|a|$, is the smallest positive integer k such that $a^k = e$. The order of a equals ∞ if such k does not exist.

Example

In $D_3 = \{\mathrm{id}, r, r^2, s, rs, r^2s\}$, $|r| = |r^2| = 3$, $|s| = |rs| = |r^2s| = 2$.

Example

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \in S_4$. Then $|\sigma| = 4$.

Example

In $\mathbb{Z}_5$, $|0| = 1$ and $|a| = 5$ if $a \neq 0$. In $\mathbb{Z}_6$, $|0| = 1$, $|1| = |5| = 6$, $|2| = |4| = 3$, $|3| = 2$.

Theorem

Let G be a group and let $a \in G$.

1. *If $|a| = \infty$, then $a^k, k \in \mathbb{Z}$, are all distinct.*
2. *If $a^i = a^j$ with $i \neq j$, then a has finite order.*
3. *If $|a| = n$, then $a^k = e$ if and only if $n \mid k$. Equivalently, $a^i = a^j \iff i \equiv j \pmod{n}$.*
4. *If $|a| = n$ and $n = td$ with $d \geq 1$, then $|a^t| = d$.*

Lemma

Let G be a group and let $a, b \in G$ be such that $|a| = m$, $|b| = n$, $\gcd(m, n) = 1$, and $ab = ba$. Then $|ab| = mn$.

Corollary (of theorem and lemma)

Let G be an Abelian group in which every element has finite order. If $c \in G$ is an element of largest order in G, then the order of every element of G divides $|c|$.

Algebraic manipulations with elements of D_n, $n \geq 3$:

Let $D_n = \{\mathrm{id}, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}$ be the dihedral group of degree n where

r : rotation counterclockwise about the origin through $\frac{2\pi}{n}$ radians.
s : reflection about the line of symmetry through vertex 1 and the origin.

Relevant properties for algebraic manipulations:

1. $r^n = \mathrm{id} = s^2 = \mathrm{id}$. Hence, $r^{-1} = r^{n-1}$ and $s^{-1} = s$.
2. $r^{-2} = r^{n-2}$ (since $r^{-2} = (r^2)^{-1}$).
3. More generally, $r^{-i} = r^{n-i}$ for any $i \in \mathbb{Z}$.
4. $sr = r^{n-1}s$, and by induction, $sr^i = r^{n-i}s$ for any $i \in \mathbb{Z}$.

Example

Calculate rsr^2s and sr^3sr^4 in

$$D_5 = \{\mathrm{id}, r, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s\}.$$

Your answers must be elements of D_5.