MTHSC 412 Section 7.2 – Basic Properties of Groups

Kevin James

Notation

We will typically represent the group operation as multiplication with identity e. However, in some cases, we will use additive notation and denote the identity by 0.

Theorem

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

1. *G has a unique identity element.*
2. $ab = ac \Rightarrow b = c$ *and* $ba = ca \Rightarrow b = c$.
3. *Each element of G has a unique inverse.*

Corollary

If G is a group and $a, b \in G$, then

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

Definition

Let G be a group with binary operation written as multiplication. For any $a \in G$ we define *nonnegative integral exponents* by

$$a^0 = e, \qquad a^1 = a, \qquad a^{n+1} = a^n a \quad n > 0.$$

Negative integral exponents are defined by

$$a^{-n} = (a^{-1})^n \qquad n > 0.$$

Definition

Let G be a group with binary operation written as addition. For any $a \in G$ we define *nonnegative integral multiples* by

$$0a = 0, \qquad 1a = a, \qquad (n+1)a = na + 1 \quad n > 0.$$

Negative integral multiples are defined by

$$(-n)a = n(-a) \qquad n > 0.$$

Theorem (Laws of Exponents)

Suppose that G is a group with binary operation denoted by multiplication and that $a, b \in G$, and $m, n \in \mathbb{Z}$. Then,

1. $x^n \cdot x^{-n} = e$,
2. $x^m \cdot x^n = x^{m+n}$,
3. $(x^m)^n = x^{mn}$, *and*
4. *If G is abelian then $(xy)^n = x^n y^n$.*

Theorem (Laws of Multiples)

Suppose that G is a group with binary operation denoted by addition and that $a, b \in G$, and $m, n \in \mathbb{Z}$. Then,

1. $nx + (-n)x = 0$,
2. $mx + nx = (m+n)x$,
3. $n(mx) = (nm)x$, *and*
4. *If G is abelian then $n(x+y) = nx + ny$.*

Definition

Suppose that G is a group. An element $a \in G$ is said to have finite order if $a^k = e$ for some $k \in \mathbb{N}$.
(If we are using additive notation then $a \in G$ has finite order if $ka = 0$ for some $k \in \mathbb{N}$.)
In this case the order of the element a denoted by $|a|$ is the smallest positive integer k such that $a^k = e$.
If there is no such positive integer then a is said to be of infinite order.

Example

1. 2 has infinite order in $\mathbb{Z}$.
2. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has infinite order in $\mathbb{GL}_2(\mathbb{Z})$.
3. The permutation represented by $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ has order 3.
4. 7 has order 2 in $U_8 = (\mathbb{Z}/8\mathbb{Z})^*$.

Theorem

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

1. *If a has infinite order, then the elements a^k, with $k \in \mathbb{Z}$ are distinct.*
2. *If $a^i = a^j$ with $i \neq j$, then a has finite order.*
3. *If $|a| = n$, then*
   1. *$a^k = e$ if and only if $n|k$.*
   2. *$a^i = a^j$ if and only if $i \equiv j \pmod{n}$.*
4. *If $|a| = n$ and $n = td$ then $|a^t| = d = \frac{n}{t}$.*
5. *If $|a| = n$ and $k \in \mathbb{Z}$, then $|a^k| = |a^{(n,k)}| = \frac{n}{(n,k)}$.*

Corollary

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