Arkansas Tech University
MATH 4033: Elementary Modern Algebra
Dr. Marcel B. Finan

14 Elementary Properties of Groups

In this section, we prove more theorems about groups. In what follows the group binary operation will be referred to as multiplication and thus we will write ab.
Several simple consequences of the definition of a group are recorded in the following two theorems.

Theorem 14.1
For any group G, the following properties hold:

(i) If $a, b, c, \in G$ and $ab = ac$ then $b = c$. (left cancellation law)
(ii) If $a, b, c, \in G$ and $ba = ca$ then $b = c$. (right cancellation law)
(iii) If $a \in G$ then $(a^{-1})^{-1} = a$. The inverse of the inverse of an element is the element itself.
(iv) If $a, b \in G$ then $(ab)^{-1} = b^{-1}a^{-1}$. That is the inverse of a product is the product of the inverses in reverse order.

Proof.
(i) Suppose that $ab = ac$. Then

$$\begin{aligned} b &= eb = (a^{-1}a)b \\ &= a^{-1}(ab) = a^{-1}(ac) \\ &= (a^{-1}a)c = ec = c \end{aligned}$$

(ii) Suppose that $ba = ca$. Then

$$\begin{aligned} b &= be = b(aa^{-1}) \\ &= (ba)a^{-1} = (ca)a^{-1} \\ &= c(aa^{-1}) = ce = c \end{aligned}$$

(iii) If $a \in G$ then since $aa^{-1} = a^{-1}a = e$ then a is an inverse of a^{-1}. Since inverses are unique then $(a^{-1})^{-1} = a$.
(iv) Let x be the inverse of ab. Then $(ab)x = e$ By associativity, we have $a(bx) = aa^{-1}$. By (i), we have $bx = a^{-1}$. But $bx = ea^{-1} = b(b^{-1}a^{-1})$ so that by applying (i) again we obtain $x = b^{-1}a^{-1}$. Therefore, $(ab)^{-1} = b^{-1}a^{-1}$.■

Theorem 14.2
If G is a group and $a, b \in G$ then each of the equations $ax = b$ and $xa = b$ has a unique solution. In the first, the solution is $x = a^{-1}b$ whereas in the second $x = ba^{-1}$.

Proof.
Consider first the equation $ax = b$. We want to isolate the x on the left side. Indeed, this can be done as follows.

$$\begin{aligned} x &= ex = (a^{-1}a)x \\ &= a^{-1}(ax) = a^{-1}b \end{aligned}$$

To prove uniqueness, suppose that y is another solution to the equation $ax = b$. Then, $ay = b = ax$. By the left cancellation property we have $x = y$. Finally, the proof is similar for the equation $xa = b$.∎

Remark 14.1
Suppose G is a finite group and $a, b \in G$. The product ax is in the row labelled by a of the Cayley table. By Theorem 14.2, the equation $ax = b$ has a unique solution means that b appears only once in the row of a of the table. Thus, each element of a finite group appears exactly once in each row of the table. Similarly, because there is a unique solution of $xa = b$, each element appears exactly once in each column of the Cayley table. It follows that each row (respectively column) is a rearrangement of the elements of the group.

Next, we discuss the extension of the associative property to products with any number of factors. More specifically, we will prove the so-called *generalized associative law* which states that in a set with associative operation, a product of factors is unchanged regardless of how parentheses are inserted as long as the factors and their order of appearance in the product are unchanged.

Definition 14.1
For elements $a_1, a_2, \cdots, a_n$ $(n \geq 2)$ of a group G define

$$a_1a_2 \cdots a_{n-1}a_n = (a_1a_2 \cdots a_{n-1})a_n.$$

Theorem 14.3 *(Generalized Associative Law)*
For any integer $1 \leq m < n$ we have

$$(a_1a_2 \cdots a_m)(a_{m+1} \cdots a_n) = a_1a_2 \cdots a_n.$$

Proof.
For $n \geq 2$, let $\mathcal{S}(n)$ be the statement

$(a_1a_2\cdots a_m)(a_{m+1}\cdots a_n) = a_1a_2\cdots a_n :$ *where* $a_1, a_2, \cdots, a_n \in G$ *and* $1 \leq m < n$.

We prove that $\mathcal{S}(n)$ is true for all $n \geq 2$ by induction on n. For $n = 2$ the statement is true since $(a_1)(a_2) = a_1a_2$ (the only possible value for m is $m = 1$.) So assume that the statement is valid for $2, 3, \cdots, n-1$. We will show that $\mathcal{S}(n)$ is also true. Suppose that $1 \leq m < n$. Then either $m = n-1$ or $1 \leq m < n-1$. If $m = n-1$ then

$$(a_1a_2\cdots a_m)(a_{m+1}\cdots a_n) = (a_1a_2\cdots a_{n-1})a_n = a_1a_2\cdots a_n.$$

So suppose that $1 \leq m < n-1$. Then

$$\begin{aligned}(a_1a_2\cdots a_m)(a_{m+1}\cdots a_n) &= (a_1a_2\cdots a_m)[(a_{m+1}\cdots a_{n-1})a_n] \\ &= [(a_1a_2\cdots a_m)(a_{m+1}\cdots a_{n-1})]a_n \\ &= (a_1a_2\cdots a_{n-1})a_n \\ &= a_1a_2\cdots a_n\end{aligned}$$

Thus, $\mathcal{S}(n)$ is true for all $n \geq 2$ and this completes a proof of the theorem. ■

Next, we introduce the concept of integral exponents of elements in a group. The concept plays an important role in the theory of cyclic groups.

Definition 14.2
For any $a \in G$ we define

$$\begin{aligned}a^0 &= e \\ a^n &= a^{n-1}a, \quad for\ n \geq 1 \\ a^{-n} &= (a^{-1})^n \quad for\ n \geq 1.\end{aligned}$$

Remark 14.2
By Theorem 14.3, $a^n = a \cdot a \cdot a \cdots a$ where the product contains n copies of a. Also, note that $aa^{n-1} = a^{n-1}a = a^n$.

The familiar laws of exponents hold in a group.

Theorem 14.4
Let a be an element of a group G and m and n denote integers. Then

(i) $a^na^{-n} = e$.
(ii) $a^ma^n = a^{m+n}$
(iii) $(a^m)^n = a^{mn}$.

Proof.
(i) The identity is trivial for $n = 0$. So suppose that $n > 0$. We use induction on n. Since $aa^{-1} = e$ then the result is true for $n = 1$. Suppose the identity holds for $1, 2, \cdots, n-1$. We must show that it is valid for n. Indeed,

$$\begin{aligned} a^n a^{-n} &= (a^{n-1}a)[(a^{-1})^{(n-1)}a^{-1}] \\ &= (aa^{n-1})[(a^{-1})^{(n-1)}a^{-1}] \\ &= [(aa^{n-1})(a^{-1})^{(n-1)}]a^{-1} \\ &= [a(a^{n-1}a^{-(n-1)})]a^{-1} \\ &= (ae)a^{-1} = aa^{-1} = e \end{aligned}$$

Thus, the identity is true for all positive integers n.
Now, suppose that $n < 0$ then

$$a^n a^{-n} = (a^{-1})^{-n}(a^{-1})^{-(-n)} = e.$$

(ii) We have to show that for a fixed integer m the identity holds for all integers n. That is, the identity holds for $n = 0, n > 0$, and $n < 0$. If $m = 0$ then $a^m a^n = a^0 a^n = ea^n = a^n = a^{0+n}$ for all integers n. So, suppose first that $m > 0$.

$\underline{n = 0}$

$$\begin{aligned} a^{m+n} &= a^{m+0} = a^m \\ a^m a^n &= a^m a^0 = a^m e = a^m \end{aligned}$$

$\underline{n > 0}$
By induction on $n > 0$. The case $n = 1$ follows from Definition 14.2. Suppose that the identity has been established for the numbers $1, 2, \cdots, n-1$. We will show that it is still true for n. Indeed,

$$\begin{aligned} a^m a^n &= a^m(a^{n-1}a) \\ &= (a^m a^{n-1})a \\ &= a^{m+n-1}a \\ &= a^{m+n} \quad (by\ Definition\ 14.2) \end{aligned}$$

By induction, it follows that the identity is true for all $n > 0$.

$\underline{n < 0, n = -m}$
Since $n = -m$ then $n + m = 0$ and in this case we have $a^{m+n} = a^0 = e$. By

(i), we have $a^m a^n = a^m a^{-m} = e$. It follows that $a^m a^n = a^{m+n}$.

$\underline{n < 0, n > -m}$
Then $m = (m + n) + (-n)$ where both $m + n$ and $(-n)$ are positive.

$$\begin{aligned} a^m a^n &= a^{(m+n)+(-n)} a^n \\ &= (a^{m+n} a^{-n}) a^n \\ &= a^{m+n} (a^{-n} a^n) \\ &= a^{m+n} e = a^{m+n} \end{aligned}$$

$\underline{n < 0, n < -m}$
In this case, $-n = m + [-(m+n)]$ where both m and $-(n+m)$ are positive.

$$\begin{aligned} a^m a^n &= a^m (a^{-1})^{-n} \\ &= a^m (a^{-1})^{m-(m+n)} \\ &= a^m [(a^{-1})^m (a^{-1})^{-(m+n)}] \\ &= a^m [a^{-m} (a^{-1})^{-(m+n)}] \\ &= (a^m a^{-m}) (a^{-1})^{-(m+n)} \\ &= (a^{-1})^{-(m+n)} = a^{m+n} \end{aligned}$$

Similar arugument holds for a fixed $m < 0$ and all integers n. This completes a proof of (ii).

(iii) Similar to (ii) and is left as an exercise.■

Remark 14.3
In the case of an group G written with the binary operation $+$, for $n \in \mathbb{Z}^+$ and $a \in G$, one writes na instead of a^n, where $na = a + ... + a$ (n times), and $(-n)a = -(na) = n(-a)$. The laws corresponding to (ii) and (iii) of Theorem 14.4 become

$$ma + na = (m + n)a$$

and

$$n(ma) = (mn)a.$$

where $m, n \in \mathbb{Z}$.

The set of all integral exponents of an element a in a group G forms a subgroup of G as shown in the next theorem.

Theorem 14.5
Let G be a group and $a \in G$. Then the set

$$< a >= \{a^n : n \in \mathbb{Z}\}$$

is a subgroup of G. In fact, $< a >$ is an Abelian Group.

Proof.
The set $< a >$ is nonempty since $a^0 = e \in < a >$. Now, let $x, y \in < a >$. Then $x = a^n$ and $y = a^m$ for some integers n and m. Thus,

$$\begin{aligned} xy^{-1} &= a^n(a^m)^{-1} \\ &= a^n a^{-m} \ (by\ Theorem\ 14.1(iv)) \\ &= a^{n-m} \ (by\ Theorem\ 14.4(ii)) \end{aligned}$$

Since $n - m \in \mathbb{Z}$ then $xy^{-1} \in < a >$. Thus, by Theorem 7.5, $< a >$ is a subgroup of G, as required. Thus, $< a >$ is itself a group. Since $a^n a^m = a^m a^n$ then $< a >$ is Abelian.■

Definition 14.3
The subgroup $< a >$ is called the **subgroup generated by a**. Any subgroup H of G that can be written as $K =< a >$ is called a **cyclic subgroup.** The element a is called a **generator**. In particular, G is a **cyclic group** if there is an element $a \in G$ such that $G =< a >$.

Example 14.1
1. The group $\mathbb{Z}$ of integers under addition is a cyclic group, generated by 1 (or -1). Thus, $(\mathbb{Z}, +)$ is a cyclic group of infinite order.
2. Let n be a positive integer. The set Z_n of congruence classes of integers modulo n is a cyclic group of order n with respect to the operation of addition with generator [1].

The following theorem shows that when powers of a are equal then the cyclic group $< a >$ is of finite order.

Theorem 14.6
Let G be a group and $a \in G$ be such that $a^r = a^s$ for some integers r and s with $r \neq s$.

(i) There is a smallest positive integer n such that $a^n = e$.

(ii) $a^t = e$ if and only if $n|t$.
(iii) The elements $e, a, a^2, \cdots, a^{n-1}$ are distinct and

$$< a >= \{e, a, a^2, \cdots, a^{n-1}\}.$$

Proof.
(i) Let $S = \{p \in \mathbb{Z}^+ : a^p = e\}$. Assume that $r > s$. (If $s > r$ then interchange the letters r and s in the following sentences) Since $a^r = a^s$ then $a^r a^{-s} = a^s a^{-s} = e$. Thus, $r - s \in S$ so that $S \neq \emptyset$ subset of $\mathbb{N}$. By Theorem 10.1, there is a smallest positive integer n such that $a^n = e$.
(ii) Suppose first that $a^t = e$ for some integer t. By the Division Algorithm there exist integers q and r such that $t = nq + r$ where $0 \leq r < n$. Thus, $e = a^t = a^{nq+r} = (a^n)^q a^r = ea^r = a^r$. By the definition of n we must have $r = 0$. That is, $t = nq$ and consequently $n|t$. Conversely, suppose that $n|t$. Then $t = nq$ for some integer q. Thus, $a^t = (a^n)^q = e$.
(iii) First we prove that $e, a, a^2, \cdots, a^{n-1}$ are all distinct. To see this, suppose that $a^u = a^v$ with $0 \leq u < n$ and $0 \leq v < n$. Without loss of generality we may assume that $u \geq v$. Since $a^u = a^v$ then $a^{u-v} = e$. By (ii), $n|(u - v)$. But $0 \leq u - v \leq u < n$. Thus, we must have $u - v = 0$ or $u = v$.
We prove $< a >= \{e, a, a^2, \cdots, a^{n-1}\}$ by double-inclusions. It is trivially true that $\{e, a, a^2, \cdots, a^{n-1}\} \subseteq < a >$. Now, let $a^t \in < a >$. By the division algorithm, there exist integers q and r such that $t = nq + r$ with $0 \leq r < n$. Thus, $a^t = (a^n)^q a^r = a^r$ with $0 \leq r < n$. That is, $a^t \in \{e, a, a^2, \cdots, a^{n-1}\}$. This completes a proof of the theorem ■

Definition 14.4
Let a be an element of a group G. The **order** of a is the smallest positive integer n, if it exists, for which $a^n = e$. If such an integer does not exist then we say that a has an **infinite order.** We denote the order of a by $o(a)$.

Example 14.2
1. In $(\mathbb{Z}_4, \oplus)$, $o([2]) = 2$.
2. In $(\mathbb{Q}^*, \cdot)$ the number 2 has infinite order since $2^n \neq 1$ for all positive integers n.

We end this section with a theorem that gives the relationship between the order of a group and the order of an element.

Theorem 14.7
If G is a group and $a \in G$ then $o(a) = | < a > |$.

Proof.
If $o(a) = n$ then by Theorem 14.6 (iii) we have $< a >= \{e, a, a^2, \cdots, a^{n-1}\}$. Thus, $| < a > | = n = o(a)$. If $o(a)$ is infinite then by Theorem 14.6(i) the integral powers of a are all distinct. Thus, $< a >$ is infinite and $o(a) = | < a > |$ ■