1 Group Theory

1.1 Definition of a Group

Definition.
Let A be a set. If $* : A \times A \to A$, then $*$ is said to be a binary operation on A.

Notation.
Let A be a set and $*$ be a binary operation on A. Let $a, b \in A$. We may write $*(a, b)$ as $a * b$.

Definition.
Let G be a group and $*$ be a binary operation on G. $(G, *)$ is said to form a group if the following are satisfied.

1. $a * (b * c) = (a * b) * c$ for any $a, b, c \in G$.
2. There exists $e \in G$ such that $a * e = e * a = a$ for any $a \in G$. e is said to be the identity element.
3. For every $a \in G$, there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$. a^{-1} is said to be the inverse of a.

Remark.
Whenever we talk about an arbitrary group $(G, *)$, we shall simply drop the binary operation $*$. So we say that G is a group and write ab instead of $a * b$.

Definition.
A group G is said to be abelian if $ab = ba$ for any $a, b \in G$.

Definition.
The order of a group G is the number of elements of G. We shall denote it by $|G|$.

1.2 Some Preliminary Lemmas

Lemma.
Let G be a group.

1. The identity element in G is unique.
2. Every $a \in G$ has a unique inverse in G.
3. For every $a \in G$, $(a^{-1})^{-1} = a$.
4. For all $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof.
Let G be a group.

1. Let e_1, e_2 be identity elements in G. Thus, since e_1 is an identity, we have $e_1e_2 = e_2$. And since e_2 is an identity, we have $e_1e_2 = e_1$. Hence, $e_1 = e_2$.
2. Let $a \in G$. Suppose a' and a'' are inverse of a. Then $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$.
3. Let $a \in G$. Let $b = a^{-1} \in G$. Then $eaa^{-1} = ab$. Hence, $b^{-1} = (ab)b^{-1}$ so that $b^{-1} = a(bb^{-1}) = ae = a$. Therefore, $(a^{-1})^{-1} = a$.
4. Let $a, b \in G$. Indeed, $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$ and $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$. ■

Lemma.
Given a, b in the group G, then the equations $ax = b$ and $ya = b$ have unique solutions for x and y in G. In particular, the two cancellation laws,

$$au = aw \text{ implies } u = w$$

and

$$ua = wa \text{ implies } u = w$$

hold in G.
Proof.
Exercise.

Problems.

1. In the following determine whether the systems described are groups. If they are not, point out which of the group axioms fail to hold.
   (a) $G = \mathbb{Z}$, $ab \equiv a - b$.
   (b) $G = \mathbb{N}$, $ab \equiv a \cdot b$, the usual product of integers.
   (c) $G = a_0, a_1, \ldots, a_6$ where $a_ia_j = a_{i+j}$ if $i + j < 7$ and $a_ia_j = a_{i+j-7}$ otherwise.
   (d) $G = \left\{ \frac{r}{s} \in \mathbb{Q} \mid (r, s) = 1, 2 \nmid s \right\}$, $ab \equiv a + b$, the usual addition of rational numbers.
2. Prove that if G is an abelian group, then for all $a, b \in G$ and all integers n, we have $(ab)^n = a^nb^n$.
3. If G is a group such that $(ab)^2 = a^2b^2$ for all $a, b \in G$, show that G musts be abelian.
4. If G is a group in which $(ab)^i = a^ib^i$ for three consecutive integers i for all $a, b \in G$, show that G is abelian. *

5. Show that the conclusion of Problem 4 does not follow if we assume the relation $(ab)^i = a^i b^i$ for just two consecutive integers.
6. In S_3 give an example of two elements x, y such that $(xy)^2 \neq x^2y^2$.
7. In S_3 show that there are four elements satisfying $x^2 = e$ and three elements satisfying $y^3 = e$.
8. If G is a finite group, show that there exists a positive integer N such that $a^N = e$ for all $a \in G$.
9. (a) If the group G has three elements, show it must be abelian.
   (b) Do part (a) if G has four elements.
   (c) Do part (a) if G has five elements.
10. Show that if every element of the group G is its own inverse, then G is abelian.
11. If G is a group of even order, prove it has an element $a \neq e$ satisfying $a^2 = e$.
12. Let G be a nonempty set closed under an associative product, which in addition satisfies:
    (a) There exists an $e \in G$ such that $ae = a$ for all $a \in G$.
    (b) Given $a \in G$, there exists an element $y(a) \in G$ such that $ay(a) = e$.

    Prove that G must be a group under this product.
13. Prove, by an example, that the conclusion of Problem 12 is false if we assume instead:
    (a) There exists an $e \in G$ such that $ae = a$ for all $a \in G$.
    (b) Given $a \in G$, there exists an element $y(a) \in G$ such that $y(a)a = e$.
14. Suppose a finite set G is closed under an associative product and that both cancellation laws hold in G. Prove that G must be a group.
15. (a) Using the result of Problem 14, prove that the nonzero integers modulo p, p a prime number, form a group under multiplication mod p.
    (b) Do part (a) for the nonzero for the nonzero integers relatively prime to n under multiplication mod n.
16. In Problem 14 show by an example that if one just assumed one of the cancellation laws, then the conclusion need not follow.
17. Prove that in Problem 14 infinite examples exist, satisfying conditions, which are not groups.
18. For any $n > 2$ construct a non-abelian group of order $2n$. (Hint: imitate the relations in S_3.)
19. If S is a set closed under an associative operation, prove that no matter how you bracket $a_1a_2 \cdots a_n$, retaining the order of the elements, you get the same element in S (e.g., $(a_1a_2)(a_3a_4) = a_1(a_2(a_3a_4))$; use induction on n).

1.3 Subgroups

Definition.
A nonempty subset H of a group G is said to be a subgroup of G if, under the product of G, H itself forms a group.

Remark.
If H is a subgroup of G and K is a subgroup of H, then K is a subgroup of G.

Lemma. Two-Step Subgroup Test.
A nonempety subset H of the group G is a subgroup of G if and only if

1. $a, b \in H$ implies that $ab \in H$.
2. $a \in H$ implies that $a^{-1} \in H$.

Proof.
If H is a subgroup of G¡, then it is obvious that (1) and (2) must hold.
Suppose conversely that H is a subset of G for which (1) and (2) hold. Since the same operation is used, associativity holds. Thus, all that remains is to prove that $e \in H$. Let $a \in H$. Then, by (2), $a^{-1} \in H$. By (1), $aa^{-1} = e \in H$. ■

Lemma.
If H is a nonempty finite subset of a group G and H is closed under multiplication, then H is a subgroup of G.
Proof.
By the previous lemma, it is enough to prove that $a^{-1} \in H$ for any $a \in H$. Suppose $a \in H$. Then since H is closed, we have that $a^2 = aa \in H$, $a^3 = a^2a \in H$, ..., $a^m \in H$, ... Thus the infinite collection $a, a^2, \ldots, a^m, \ldots$ is contained in H, which is finite. Thus there must be repetitions in this collection, i.e. there are integers r, s such that $r > s > 0$

and $a^r = a^s$. By the cancellation in G, $a^{r-s} = e$. Hence, $a^0 = e \in H$. Thus, we have $r - s - 1 \geq 0$ so that $a^{r-s-1} \in H$. Also, $aa^{r-s-1} = a^{r-s} = e$ so that $a^{r-s-1} = a^{-1}$, so that $a^{-1} \in H$. ■

Definition.
Let G be a group, H be a subgroup of G; for $a, b \in G$; for $a, b \in G$ we say that a is congruent to b mod H, written as $a \equiv b \mod H$, if $ab^{-1} \in H$.

Lemma.
The relation $a \equiv b \mod H$ is an equivalence relation.
Proof.
First, note that $e \in H$ since H is a subgroup of G. Hence, $aa^{-1} \in H$ so that $a \equiv a \mod H$.
Next, suppose that $a \equiv b \bmod H$. Then $ab^{-1} \in H$. Since H is a group, $(ab^{-1})^{-1} \in H$. But $(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1}$ so that $b \equiv a \bmod H$.
Now, suppose that $a \equiv b \mod H$ and $b \equiv c \mod H$. Then $ab^{-1} \in H$ and $bc^{-1} \in H$ so that $(ab^{-1})(bc^{-1}) \in H$. But $(ab^{-1})(bc^{-1}) = a(b^{-1}b)c^{-1} = aec^{-1} = ac^{-1}$, so that $ac^{-1} \in H$. Hence, $a \equiv c \mod H$. ■

Definition.
If H is a subgroup of G, $a \in G$, then $Ha = \{ha \mid h \in H\}$. Ha is called a right coset of H in G.

Lemma.
For all $a \in G$, $Ha = \{x \in G \mid a \equiv x \mod H\}$.
Proof.
Let $[a] = \{x \in G \mid a \equiv x \bmod H\}$. We first show that $Ha \subseteq [a]$. For, if $h \in H$, then $a(ha)^{-1} = a(a^{-1}h^{-1}) = h^{-1} \in H$ since H is a subgroup of G. Thus, $a \equiv ha \bmod H$ so that $ha \in [a]$. Thus, $Ha \subseteq [a]$.
Now, suppose that $x \in [a]$. Hence, $ax^{-1} \in H$. Since H is a subgroup of G, $(ax^{-1})^{-1} \in H$. But $(ax^{-1})^{-1} = xa^{-1}$. Thus, $xa^{-1} \in H$ so that $xa^{-1}a \in Ha$. Hence, $x \in Ha$. Therefore, $[a] \subseteq Ha$. ■

Lemma.
There is a one-to-one correspondence between any two right cosets of H in G.
Proof.
Let H be a subgroup of G and $a, b \in G$. Define a function $\phi : Ha \to Hb$ by $\phi(ha) = hb$ for every $h \in H$. If $hb \in Hb$ then $ha \in Ha$ and $\phi(ha) = hb$ so that ϕ is onto. Now, suppose that $\phi(h_1a) = \phi(h_2a)$. Then $h_1b = h_2b$ and thus, by cancellation in G, $h_1 = h_2$. Hence, $h_1a = h_2a$ so that ϕ is one-to-one. Therefore, there is a one-to-one correspondence between Ha and Hb, and since a and b are arbitrary, there is a one-to-one correspondence between any two right cosets of H in G. ■

Theorem. Theorem of Lagrange.
If G is a finite group and H is a subgroup of G, then $|H| \mid |G|$.
Proof.
First, note that $H = He$ so that H is a coset of itself in G. By the previous two lemmas, we have that any two distinct right cosets of G are disjoint and that each of these distinct right cosets has $|H|$ elements. Now, consider $S = \bigcup_{a \in G} Ha$. Clearly, for any $h \in H$ and any $a \in G$, we have that $ha \in G$ so that any right coset of H in G is a subset of G. Also, any $a \in G$ is in the right coset Ha since $e \in H$. Thus, G is a subset of S. Hence, $G = S$. Hence, $|G| = |S|$. But $|S| = k|H|$ since S is a union of k disjoint sets with $|H|$ elements each, where k is the number of distinct right cosets of H in G. Hence, $|G| = k|H|$ so that $|H| \mid |G|$. ■

Definition.
If H is a subgroup of G, the index of H in G is the number of distinct right cosets of H in G.

Definition.
If G is a group and $a \in G$, the order (or period) of a is the least positive integer m such that $a^m = e$. We shall denote it by $|a|$. If no such integer exists, we say that a is of infinite order.

Definition.
Let G be a group and $a \in G$. The cyclic subgroup generated by a, denoted by $\langle a \rangle$
Corollary.
If G is a finite group and $a \in G$, then $|a|$ divides $|G|$.

Proof.