Groups

Definition (reminder) If $n \in \mathbb{N}$ then for $a, b \in \mathbb{Z}$ we define the equivalence relation $\equiv_n$ on $\mathbb{Z}$ as follows: $a \equiv_n b$ if and only if $n|(b-a)$; $\mathbb{Z}_n$ denotes the equivalence classes: $\mathbb{Z}_n = \{[x]_n | x \in \mathbb{Z}\}$.

Theorem 9.0. Define the operation $+_n$ and $\cdot_n$ on $\mathbb{Z}$ as follows:

$$[x]_n +_n [y]_n = [x+y]_n$$

$$[x]_n \cdot_n [y]_n = [x \cdot y]_n$$

Then the operations $+_n$ and $\cdot_n$ are well defined.

Exercise. Consider the objects $\mathbb{Z}_4, \mathbb{Z}_5, \mathbb{Z}_6, \mathbb{Z}_7$ with the operations $+_n$ and $\cdot_n$. Construct the addition and multiplication "tables". We will be making heavy use of these objects.

A group is a set of elements G with an operation $\cdot$ that has the following properties:

1. Closure: if $x \in G$ and $y \in G$ then
   $x \cdot y \in G$;
2. Associativity: if $x, y, z \in G$ then
   $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;
3. Identity: there is an element $e \in G$ so that for each $x \in G$:
   $e \cdot x = x = x \cdot e$;
4. Inverses: for each $x \in G$ there is an element x^{-1} so that
   $x \cdot x^{-1} = e = x^{-1} \cdot x$.

Theorem 9.1 [Uniqueness of the identity]. Suppose that G is a group with identity e. If $\hat{e}$ is an element of G so that for all $x \in G$, $\hat{e}x = x = x\hat{e}$ then $e = \hat{e}$.

Theorem 9.2 [Uniqueness of the inverse]. Suppose that G is a group with identity e and $x \in G$. Then there is a unique element $x' \in G$ so that $x \cdot x' = x' \cdot x = e$. [Notation: the unique inverse of the element x is denoted by x^{-1}.]

Theorem 9.3. Suppose that G is a group and $x, y, z \in G$ are arbitrary elements. Then:

1. $(x^{-1})^{-1} = x$.
2. $(xy)^{-1} = y^{-1}x^{-1}$.
3. $(xy = xz) \Rightarrow (y = z)$.
4. $(yx = zx) \Rightarrow (y = z)$.

Example 9.1. Let $S = \{1, 2, 3, \ldots, n\}$ define S_n to be the collection of all 1-to-1 functions of S onto itself. Define the operation $\circ$ between the elements $\alpha, \beta \in S_n$ by ordinary composition, thus for each $s \in S$ we have $(\alpha \circ \beta)(x) = \alpha(\beta(x))$. The set S_n with the operation $\circ$ is a group.

Definition. A group G is said to be Abelian (or to be a commutative group) if and only if $xy = yx$ for all $x, y \in G$.

Exercise 9.1. Construct the multiplication charts for the groups S_2 and S_3. Are these groups Abelian?

Exercise 9.2. How many elements are in the groups S_4 and S_5. Show that these groups are not Abelian and that each one of these has a "subgroup" equivalent to S_3.

Definition. Suppose that G is a group with operation $\cdot$ and $H \subset G$. Then H is said to be a subgroup of G if H with the operation $\cdot$ is a group.

Exercise 9.3. We would like to determine when the following sets with the indicated operations are groups, assume n is an integer with $n > 1$:

$$\begin{array}{rcc} \mathbb{Z}_n & \text{with operation} & + \quad \text{mod } n \\ \mathbb{Z}_n - \{[0]\} & \text{with operation} & \cdot \quad \text{mod } n. \end{array}$$

Look at examples for $n = 6, 7, 10, 11$. Which of these yield groups (it's not necessary to write out the whole table to answer this question.) (And why was 0 removed from the set?)

Theorem 9.4. Suppose that G is a group with operation $\cdot$ and $H \subset G$ and it it true that for $h_1, h_2 \in H$ we have $h_1 \cdot h_2^{-1} \in H$. Then H is a subgroup of G.

Notational conventions. When working with the set $\mathbb{Z}_n$, then I will frequently omit the brackets $[x]_n$ when it is understood that we are working with $\mathbb{Z}_n$; and operations $+_n$ and $\cdot_n$ are often denoted by $+$ mod n or $\cdot$ mod n respectively. Thus following are equivalent ways of writing the same thing:

$$\begin{aligned} x \equiv_n y &\quad\Leftrightarrow\quad x = y \bmod n \\ [3]_5 +_5 [4]_5 = [2]_5 &\quad\Leftrightarrow\quad 3 + 4 = 2 \bmod 5. \end{aligned}$$

Exercise 9.4. Find all the subgroups of $(\mathbb{Z}_6, + \mod 6)$ and of $(\mathbb{Z}_7 - \{[0]\}, \times \mod 7)$.

Definition. For $\mathbb{Z}_n$ I want to be able to define the quantity $[b] = [a]^{[x]}$. Unlike the addition and multiplication operators this is not naturally well-defined. (In fact if $x < 0$ then a^x is not even an integer.) So we define it as follows: if whenever $x, y > 0$ we have that $x \equiv_n y \Rightarrow a^x \equiv a^y$ then we define $[b]_n = [a^x]_n$. When it is defined, we can let $[a^x]$ denote $[b]$ for positive integers x.

Definition. Suppose that each of G and H are groups with operations $\otimes$ and $\boxtimes$ respectively and that $\varphi : G \to H$ is a function. Then φ is called a *homomorphism* if the following holds for all $x, y \in G$:

$$\varphi(x \otimes y) \quad = \quad \varphi(x) \boxtimes \varphi(y).$$

A homomorphism that is 1-to-1 is called an *isomorphism*.

Exercise 9.5 Determine which of the following functions are well-defined, if so are they homomorphisms: (Note that I am abbreviating the elements of the groups so that, for example in a: x means $[x]_6$, $\varphi(x)$ means $[\varphi(x)]_{12}$.) Are they isomorphisms?

a.	$\varphi(\mathbb{Z}_6, +_6) \to (\mathbb{Z}_{12}, +_{12})$	with	$\varphi(x) = 2x \bmod 12$
b.	$\varphi(\mathbb{Z}_6, +_6) \to (\mathbb{Z}_{10}, +_{10})$	with	$\varphi(x) = 2x \bmod 10$
c.	$\varphi(\mathbb{Z}_6, +_6) \to (\mathbb{Z}_7 - \{0\}, \cdot_7)$	with	$\varphi(x) = 3^x \bmod 7$
d.	$\varphi(\mathbb{Z}_6, +_6) \to (\mathbb{Z}_7 - \{0\}, \cdot_7)$	with	$\varphi(x) = 2^x \bmod 7$
e.	$\varphi(\mathbb{Z}_6, +_6) \to (\mathbb{Z}_7 - \{0\}, \cdot_7)$	with	$\varphi(x) = 5^x \bmod 7$
f.	$\varphi(\mathbb{Z}_{12}, +_{12}) \to (\mathbb{Z}_6, +_6)$	with	$\varphi(x) = x \bmod 6$

Notation. If G is a group with identity element e and $g \in G$ then:

i. g^0 denotes e;

ii. g^1 denotes g;

iii. for a positive integer $n > 1$, g^n is defined inductively as:

$$g^n = g^{n-1} \cdot g.$$

Theorem 9.5. Suppose that G is a group with the usual notation for the operation. Then:

$$\begin{array}{lll} a. & (g^{-1})^n = (g^n)^{-1} & \text{for } g \in G, n \in \mathbb{Z}^+ \\ b. & g^n \cdot g^m = g^{n+m} & \text{for } g \in G, n, m \in \mathbb{Z}^+ \end{array}$$

Exercise 9.6. Prove that if G is a group and $g \in G$ then $H = \{g^n | n \in \mathbb{Z}\}$ is a subgroup of G. Note: H is called a *cyclic subgroup* of G; if there is an element of $g \in G$ so that the corresponding subgroup H is all of G then G is called a *cyclic* group.

Theorem 9.6. Suppose that G is a group and H is a subgroup of G. Define the relation $\sim$ on G by $g \sim h$ if and only if $gh^{-1} \in H$. Then:

a. $\sim$ is an equivalence relation on G.

b. Let $p \in G$ and define $Hp = \{hp | h \in H\}$; then the function $f : H \to Hp$ defined by $f(h) = hp$ is 1-to-1 and onto. Definition: the set Hp is a called the *right coset* of H generated by p.

c. $[e]_\sim = H$.

d. The collection $\{Hg | g \in G\}$ is a partition of G.

Exercise 9.7. Consider $G = (\mathbb{Z}_{12}, +)$. Let $H = \{0, 3, 6, 9\}$.

a. Show that H is a subgroup of G.

b. Find all the cosets of H in G and denote this set by G/H.

[Note: If $x \in G$ then $H +_{12} [x]_{12} = \{[h + x]_{12} \big| [h]_{12} \in H\}$ is the coset generated by x.]

c. For $H +_{12} [x]_{12}, H +_{12} [y]_{12} \in G/H$ define $(H +_{12} [x]_{12}) \oplus (H +_{12} [y]_{12})$ by $(H +_{12} [x]_{12}) \oplus (H +_{12} [y]_{12}) = H +_{12} [x + y]_{12}$.

d. Show that $\oplus$ is well defined and construct the addition table for G/H with the operation $\oplus$.

Let $\varphi : G \to G/H$ be defined by $\varphi(x) = H +_{12} [x]_{12}$.

e. Is φ well defined?

f. Is φ 1-1 and/or onto?

g. Is φ a homomorphism? - an isomorphism?

Corollary to 9.6 [Lagrange's theorem]. If G is a group and H is a subgroup of G then $|H| \Big| |G|$.

Theorem 9.7. Suppose that G is a group and $g \in G$. Then the set $H = \{h | gh = hg\}$ is a subgroup of G.

Theorem 9.8. Suppose that G is a group. Let $H = \{h \in G | gh = hg \text{ for all } g \in G\}$ is a subgroup of G. (This is called the commutator subgroup of G and is the set all elements that commute with all the elements of G.)

Theorem 9.10. Suppose that G_1 and G_2 are groups and $\varphi : G_1 \to G_2$ is a homomorphism. Then $h(e_1) = e_2$ where e_1 is the identity element of G_1 and e_2 is the identity element of G_2.

Exercise 9.8. Consider the group $(\mathbb{Z}_n, +_n)$ with the operation of addition mod n. Suppose that H is a subgroup of $\mathbb{Z}_n$. Let J be the collection of all cosets of H in $\mathbb{Z}_n$. Define the operation $\oplus$ on J as follows:

$$(H +_n x) \oplus (H +_n y) = H +_n (x +_n y).$$

Define the operation $\boxplus$ as follows: if H_1 and H_2 are two cosets then

$$H_1 \boxplus H_2 = \{x +_n y | x \in H_1, y \in H_2\}.$$

Show that:

a. $\oplus$ is well defined.

b. $H_1 \boxplus H_2 = H_1 \oplus H_2$.

b. J with the operation $\oplus$ is a group.

c. J is abelian.

d. $|H| \cdot |J| = n$.

Exercise 9.9. Prove that a group G is abelian if and only if $(xy)^2 = x^2 y^2$ for all $x, y \in G$.