Section I.1. Semigroups, Monoids, and Groups

Note. In this section, we review several definitions from Introduction to Modern Algebra (MATH 4127/5127). In doing so, we introduce two algebraic structures which are weaker than a group. For background material, review John B. Fraleigh's *A First Course in Abstract Algebra*, 7th Edition, Addison-Wesley/Pearson Education (2003), Sections 2, 3, and 4. For more details, see my online notes for Introduction to Modern Algebra.

Definition. If G is a nonempty set, then a *binary operation* on G is a function from $G \times G$ to G. If the binary operation is denoted $*$, then we use the notation $a * b = c$ if $(a, b) \in G \times G$ is mapped to $c \in G$ under the binary operation.

Note. We will consider both "additive" and "multiplicative" binary operations. The only difference between these operations is notational, really. When considering a binary operation, we denote the image of (a, b) as $a + b$. When using multiplicative notation, we denote the image of (a, b) as ab (called the *product* of a and b). Throughout this first chapter we use multiplicative notation.

Definition I.1.1. For a multiplicative binary operation on $G \times G$, we define the following properties:

(i) Multiplication is *associative* if $a(bc) = (ab)c$ for all $a, b, c, \in G$.

(ii) Element $e \in G$ is a two-sided *identity* if $ae = ea = a$ for all $a \in G$.

(iii) Element $a \in G$ has a two-sided *inverse* if for some $a^{-1} \in G$ we have $aa^{-1} = a^{-1}a = e$.

A *semigroup* is a nonempty set G with an associative binary operation. A *monoid* is a semigroup with an identity. A *group* is a monoid such that each $a \in G$ has an inverse $a^{-1} \in G$. In a semigroup, we define the property:

(iv) Semigroup G is *abelian* or *commutative* if $ab = ba$ for all $a, b \in G$.

The *order* of a semigroup/monoid/group is the cardinality of set G, denoted $|G|$. If $|G| < \infty$, then the semigroup/monoid/group is said to be *finite*.

Note. If we define a *binary algebraic structure* as a set with a binary operation on it, then we have the following schematic:

$$(\text{Binary Algebraic Structures}) \supseteq (\text{Semigroups}) \supseteq (\text{Monoids}) \supseteq (\text{Groups}).$$

Note. The following result is standard and we leave a detailed proof as a homework exercise.

Theorem I.1.2. If G is a monoid, then the identity element e is unique. If G is a group then:

(*i*) If $c \in G$ and $cc = c$ then $c = e$.

(*ii*) For all $a, b \in G$, if $ab = ac$ then $b = c$, and if $ba = ca$ then $b = c$ (these properties of a group is called *left cancellation* and *right cancellation*, respectively).

(*iii*) For $a \in G$ the inverse of a, a^{-1}, is unique.

(*iv*) For all $a \in G$, we have $(a^{-1})^{-1} = a$.

(*v*) For all $a, b \in G$ we have $(ab)^{-1} = b^{-1}a^{-1}$.

(*vi*) For all $a, b \in G$, the equations $ax = b$ and $ya = b$ have unique solutions in G, namely $x = a^{-1}b$ and $y = ba^{-1}$, respectively.

Note. We can weaken the two-sided identity and inverse properties used in Definition 1.1 of group. It turns out that if we simply assume right inverses and a right identity (or just left inverses and a left identity) then this implies the existence of left inverses and a left identity (and conversely), as shown in the following theorem (and in Exercise 4.38 of Fraleigh).

Proposition I.1.3. Let G be a semigroup. Then G is a group if and only if the following conditions hold.

(i) There exists an element $e \in G$ such that $ea = a$ for all $a \in G$ (called a *left identity* in G).

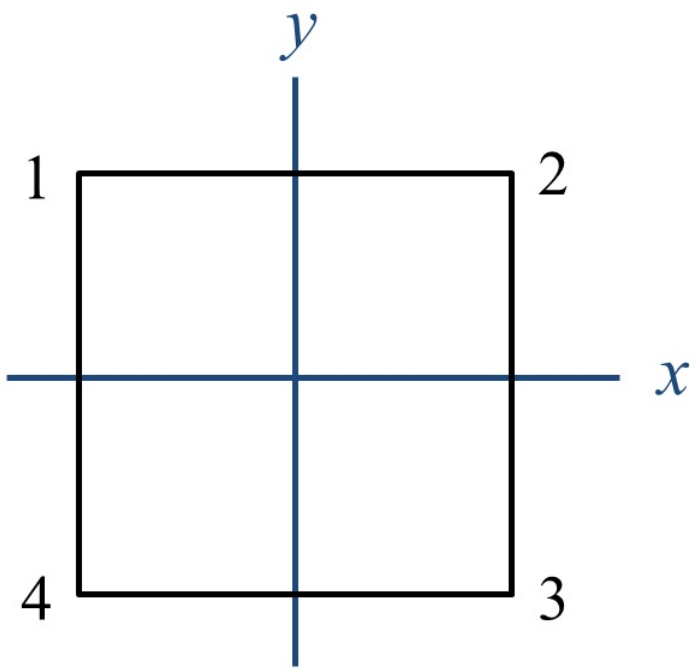
(ii) For each $a \in G$, there exists an element $a^{-1} \in G$ such that $a^{-1}a = e$ (a^{-1} is called a *left inverse* of a).

Note. The following proposition gives another condition by which a semigroup is a group.

Proposition I.1.4. Let G be a semigroup. Then G is a group if and only if for all $a, b \in G$ the equations $ax = b$ and $ya = b$ have solutions in G.

Example. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ form infinite abelian groups under addition. Each is an abelian monoid under multiplication, but not a group (since 0 has no multiplicative inverse). The set of all 2×2 matrices with real entries form a nonabelian monoid under matrix multiplication but not a group (since this set includes many singular matrices). The nonzero elements of $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ form infinite abelian groups under multiplication (denoted $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$, respectively). The even integers under multiplication form an abelian semigroup that is not a monoid (since it contains no multiplicative identity).

Example. Hungerford describes the group D_4^* of transformations of a square (i.e., the "group of symmetries" of a square) by considering the picture



and the transformations $\{I, R, R^2, R^3, T_x, T_y, T_{1,3}, T_{2,4}\}$ where I is the identity transformation, R is a counterclockwise rotation through $90°$, R^2 is a counterclockwise rotation through $180°$, R^3 is a counterclockwise rotation through $270°$, T_x is a reflection about the x axis, T_y is a reflection about the y axis, $T_{1,3}$ is a reflection about the line through the points labeled 1 and 3, and $T_{2,4}$ is a reflection about the line through the points labeled 2 and 4. The binary operation on these transformations is simply the application of one transformation U followed by another V, denoted $U * V$. For example, consider $R * T_x$. In terms of the images of the labeled points we have $R * T_x(1) = R * (T_x(1)) = R(4) = 3$, $R * T_x(2) = R * (T_x(2)) = R(3) = 2$, $R * T_x(3) = R * (T_x(3)) = R(2) = 1$, $R * T_x(4) = R * (T_x(4)) = R(1) = 4$, so $R * T_x = T_{2,4}$ (notice that in the table we give entries $U * V$ where U is from the leftmost column and V is from the top row). Notice from the table that $\{I, R, R^2, R^3\}$

forms a subgroup of order 4 of D_4^*. We will define the general dihedral group D_n in Section I.6 and do so using cycles in a permutation group.

The multiplication table for group D_4^* is (this is Exercise I.1.4):

$*$	I	R	R^2	R^3	T_x	T_y	$T_{1,3}$	$T_{2,4}$
I	I	R	R^2	R^3	T_x	T_y	$T_{1,3}$	$T_{2,4}$
R	R	R^2	R^3	I	$T_{2,4}$	$T_{1,3}$	T_x	T_y
R^2	R^2	R^3	I	R	T_y	T_x	$T_{2,4}$	$T_{1,3}$
R^3	R^3	I	R	R^2	$T_{1,3}$	$T_{2,4}$	T_y	T_x
T_x	T_x	$T_{2,4}$	T_y	$T_{1,3}$	I	R^2	R	R^3
T_y	T_y	$T_{1,3}$	T_x	$T_{2,4}$	R^2	I	R^3	R
$T_{1,3}$	$T_{1,3}$	T_y	T_x	$T_{2,4}$	R^3	R	I	R^2
$T_{2,4}$	$T_{2,4}$	T_x	$T_{1,3}$	T_y	R	R^3	R^2	I

Example/Definition. Let S be a nonempty set and $A(S)$ the set of all bijections from S to S. Then $A(S)$ forms a group under function composition. $A(S)$ is the group of *permutations* on set S. If $S = \{1, 2, \ldots, n\}$ then $A(S)$ is the *symmetric group on n letters*, denoted S_n. The order of S_n is $|S_n| = n!$ (Exercise I.1.5).

Note. We often denote elements of S_n by listing the elements of $S = \{1, 2, \ldots, n\}$ in the first row of a $2 \times n$ matrix listing the corresponding images in the second row of the matrix: $\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ where $\alpha(k) = i_k$ for $1 \leq k \leq n$. We then compose two permutations by applying one after the other. For example,

consider $\sigma, \tau \in S_4$ where $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$. We denote the product $\sigma\tau$ as the result of applying τ first and then σ to the set S (think of this as τ "acting on" set S and the σ "acting on" the result; so, as in the usual function composition, $\sigma\tau(S) = \sigma(\tau(S))$), This means that to compute $\sigma\tau$ we must read from right to left to get

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}.$$

Notice that

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

and so $\sigma\tau \neq \tau\sigma$ and S_4 is not abelian (nor, of course, is S_n for $n \geq 3$). This notation of reading right to left is not universal, but it is the same notation as used in Fraleigh (see Section II.8).

Definition. Let G and H be multiplicative groups. Define the *direct product* of G and H as $G \times H = \{(g, h) \mid g \in G, h \in H\}$ with the binary operation $(g, h)(g', h') = (gg', hh')$. Similarly, if G and H are additive groups, we denote this as $G \oplus H$ and call it the *direct sum*.

Note. If e_G and e_H are the identities of groups G and H, respectively, then the identity of $G \times H$ is (e_G, e_H). For $(g, h) \in G \times H$, the inverse is $(g, h)^{-1} = (g^{-1}, h^{-1})$.

Note. The following result introduces equivalence relations on monoids. This is our first step on the way to considering cosets and quotient groups (to be continued in Section I.4).

Theorem I.1.5. Let $R(\sim)$ be an equivalence relation on a monoid G such that $a_1 \sim a_2$ and $b_1 \sim b_2$ imply $a_1b_1 \sim a_2b_2$ for all $a_i, b_i \in G$. Such an equivalence relation on G is called a *congruence relation* on G. Then the set G/R of all equivalence classes of G under R is a monoid itself under the binary operation defined by $(\overline{a})(\overline{b}) = \overline{ab}$, where $\overline{x}$ denotes the equivalence class containing x. If G is a group, then so is G/R. If G is abelian, then so is G/R.

Example. Probably the most familiar equivalence relation to you is equivalence modulo m on $\mathbb{Z}$. That is, for $a, b \in \mathbb{Z}$ we say that $a \sim b$ if an only if $a \equiv b \pmod{m}$ (where $m \in \mathbb{N}$). Let $\mathbb{Z}_m$ be the set of all equivalence classes resulting from $\sim$: $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$. Then $\mathbb{Z}_m$ is an additive abelian group of order m. In fact, $\mathbb{Z}_p \setminus \{\overline{0}\}$ forms a multiplicative group of order $p-1$ when p is prime (Exercise I.1.7).

Example. Another useful example of a group which involves equivalence classes is based on the relation $\sim$ on $\mathbb{Q}$, where, for $a\, b \in \mathbb{Q}$, $a \sim b$ if and only if $a-b \in \mathbb{Z}$. Then $\sim$ is a congruence relation by Exercise I.1.8. By Theorem I.1.5 the set of equivalence classes, which we denote $\mathbb{Q}/\mathbb{Z}$, form an additive group where, for $\overline{a}, \overline{b} \in \mathbb{Q}/\mathbb{Z}$, we take $\overline{a} + \overline{b} = \overline{a+b}$. This is called the *group of rationals modulo one*. An important group in the theory of infinite abelian groups is the Prüfer group (named for Heinz Prüfer [1896–1934]), $Z(p^\infty)$, defined in Exercise I.1.10; it is a subgroup of $\mathbb{Q}/\mathbb{Z}$.

Note. We want to put a meaning on taking a product of several elements of a monoid G: For $a_1, a_2, \ldots, a_n \in G$, define $a_1 a_2 \cdots a_n \in G$. Since the operation of G is a *binary* operation, this product must be given a meaning based on multiplication of two elements at a time. With only 3 elements we have by associativity that $(a_1 a_2)a_3 = a_1(a_2 a_3)$ and there can be no ambiguity. But with many elements, it is not obvious that different groupings don't yield different results for the product (though we expect associativity to help in this general case as well). We now prove some results on these products before moving on in our study of groups.

Definition. Given any sequence of elements of a semigroup G, $\{a_1, a_2, \ldots, a_n\}$ define a *meaningful product* of $a_1, a_2, \ldots, a_n$ in this order as:

(1) If $n = 1$ the product is a_1.

(2) If $n > 1$ then define a meaningful product to be any product of the form $(a_1 a_2 \cdots a_m)(a_{m+1} a_{m+2} \cdots a_n)$ where $m < n$ and $(a_1 a_2 \cdots a_m)$ and $(a_{m+1} a_{m+2} \cdots a_n)$ are meaningful products of m and $n - m$ elements, respectively.

Note. We need the Strong Principle of Mathematical Induction to show that the meaningful product as given in (2) is well-defined (Hungerford refers to the Recursion Theorem in a footnote here; the Recursion Theorem is just basic mathematical induction).

Definition. Given any sequence of elements of a semigroup G, $\{a_1, a_2, \ldots, a_n\}$ define the *standard n product* $\prod_{i=1}^{n} a_i$ of $a_1, a_2, \ldots, a_n$ as follows:

$$\prod_{i=1}^{1} a_i = a_1; \text{ for } n > 1, \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i \right) a_n.$$

Note. We only need the Principle of Mathematical Induction (or Hungerford's Recursion Theorem, Theorem 6.2, of the Introduction) to show that the standard meaningful product is well-defined. The following result shows that meaningful products are the proper way to unambiguously define the product of several elements of a semigroup. Notice that in the proof of the following, we reserve the product notation "$\prod$" for the standard n product.

Theorem I.1.6. Generalized Associative Law.

If G is a semigroup and $a_1, a_2, \ldots, a_n \in G$ then any two meaningful products of $a_1, a_2, \ldots, a_n \in G$ in this order are equal.

Note. The Generalized Associative Law allows us to write a product of several elements without concern over inserting parentheses to produce pairs of elements.

Note. The following result also concerns products of several elements but involves commutivity. It can also be proved using induction.

Corollary I.1.7. Generalized Commutative Law.
If G is a commutative semigroup and $a_1, a_2, \ldots, a_n \in G$ then for any permutation $i_1, i_2, \ldots, i_n$ of $i = 1, 2, \ldots, n$ we have the products $a_1 a_2 \cdots a_n = a_{i_1} a_{i_2} \cdots a_{i_n}$.

Note. The following definition makes clear what it means to repeatedly apply the binary operation to a single element (that is, to raise an element to a power, in the multiplicative notation case).

Definition I.1.8. Let G be a (multiplicative) semigroup, $a \in G$, and $n \in \mathbb{N}$. The element a^n is defined as the standard n product $a^n = \prod_{i=1}^{n} a_i$ where $a = a_i$ for $1 \leq i \leq n$. If G is a monoid, a^0 is defined to be the identity element of G, $a^0 = e$. If G is a group, then for each $n \in \mathbb{N}$, a^{-n} is defined to be $a^{-n} = (a^{-1})^n \in G$. If G is an additive group we replace a^n, a^0, a^{-n}, and e with na, $0a$, $-na$, and 0, respectively.

Note. The following is unsurprising and we omit the proof.

Theorem I.1.9. If G is a group (respectively, semigroup, monoid) and $a \in G$, then for all $m, n \in \mathbb{Z}$ (respectively, $\mathbb{N}$, $\mathbb{N} \cup \{0\}$):

(i) $a^m a^n = a^{m+n}$ (or $ma + na = (m + n)a$ in additive notation);

(ii) $(a^m)^n = a^{mn}$ (or $n(ma) = (mn)a$ in additive notation).