Semigroups, monoids, groups and rings
(Optional reading)

1 Semigroups

A *semigroup* a set with an associative binary operation (multiplication). The associative law states that $(ab)c = a(bc)$ holds for any three elements a, b, c. This law allows us to define a^n for all positive integer n as the product of n copies of a, without specifying the grouping of the elements. A semigroup is *commutative* if it satisfies $ab = ba$ for any pair of elements.

An element z is a *left zero* if $za = z$ holds for all a, and it is a *right zero* if $az = z$ holds for a. There may be infinitely many left zeroes or right zeroes: for example on any set S we may define a *left zero semigroup* by the rule $ab = a$. This rule defines an associative multiplication, since we have $a(bc) = ab = a = ac = (ab)c$. Every element of a left zero semigroup is a left zero. An element is a *zero element* if it is a left zero and also a right zero. If there is a zero element, then it is unique. Actually a stronger statement is true: any left zero element is equal to any right zero element. If z_ℓ is a left zero and z_r is a right zero then

$$z_\ell = z_\ell z_r = z_r.$$

An element e is a *left identity* if $ea = a$ holds for all a and it is a *right identity* if $ae = a$ holds for all a. There may be infinitely many right identities: for example, every element of a left zero semigroup is a right identity. That said, if a semigroup has a left identity e_ℓ and and also a right identity e_r , then the two are equal:

$$e_\ell = e_\ell e_r = e_r.$$

An element is an *identity element* if it is a right identity and also a left identity. The identity element in a semigroup is unique.

2 Monoids

The definition of a monoid is motivated by the following example. Consider the semigroup on the set $\{1, e, f\}$ given by the following multiplication table.

$\times$	1	e	f
1	1	e	f
e	e	e	f
f	f	f	f

The identity element of this semigroup is 1. Note that the subset $\{e, f\}$ is a subsemigroup, the element e is the multiplicative identity of this subsemigroup, but it is not the identity element of the larger semigroup. Algebraists found this confusing and, as a workaround, made the following definition. A *monoid* is a set with two operations: one is an associative binary operation, and the other is a distinguished constant 1 which must satisfy $1 \cdot a = a \cdot 1 = a$ for every element of the monoid. We can think of a distinguished constant as a zero variable operation, and the rule $1 \cdot a = a \cdot 1 = a$ is just another rule (postulating that the distinguished constant must be the multiplicative identity). Every submonoid of a monoid must contain its distinguished constant. In the above example, the set $\{e, f\}$ is a subsemigroup with respect to multiplication, but it is not a submonoid, if we fix 1 as the distinguished identity element.

Whether we introduce monoids, or just refer to an (the) identity element of a semigroup, we can define inverses whenever there is an identity element: b is a *right inverse* of a if $ab = 1$ holds and c is a *left inverse of* a if $ca = 1$ holds. There may be infinitely many left inverses and right inverses. To show this consider the set of all functions $f : \mathbb{Z} \to \mathbb{Z}$, with respect to composing functions: $f \circ g(x)$ is defined to be $f(g(x))$. This is a semigroup since composing functions is associative: $f \circ (g \circ h)(x) = f((g \circ h)(x)) = f(g(h(x)) = f \circ g(h(x)) = (f \circ g) \circ h(x)$ holds for all $x \in \mathbb{Z}$. It also has a (two-sided) identity element: the identity function, given by $\iota(x) = x$ for all x satisfies $f \circ \iota = \iota \circ f = f$ for all f.

Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = 2x$. This function is injective (if $2x_1 = 2x_2$ then $x_1 = x_2$) but not surjective (only even integers are in the range). It has infinitely many left inverses: any function g that sends each even x into $x/2$ satisfies $g \circ f = \iota$. (We may freely choose the values of $g(1)$, $g(3)$, $g(5)$ etc.)

Consider now the function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = \lfloor x/2 \rfloor$. This function is surjective: any $x \in \mathbb{Z}$ satisfies $f(2x) = x$, but it is not injective: $f(2) = f(3) = 1$.

It is easy to show for any set X and the set of functions $f : X \to X$ with the composition operation that a function f has a left inverse if and only if it is injective and it has a right inverse if and only if it is surjective.

It is true for monoids (or semigroups with an identity element) that whenever an element a has a right inverse u and a left inverse v then they are equal: if $au = 1$ and $va = 1$ then

$$v = v \cdot 1 = v(au) = (va)u = 1 \cdot u = u.$$

Hence the two-sided inverse (if it exists) is unique.

3 Groups

A *group* is a monoid (or semigroup with an identity element) in which every element has an inverse. A group is *commutative* if the multiplication is commutative. We often use the *additive notation* for commutative groups: we write $a+b$ instead of ab. In this case the additive identity element is denoted by 0 and the additive inverse of a is $-a$. When we use the additive notation, we refer to the group as an *Abelian group*

It is easy to show in a group that $(a^{-1})^{-1} = a$ holds for all a and that $(ab)^{-1} = b^{-1}a^{-1}$ holds for any pair of elements. As a consequence, for Abelian groups we have $-(-a) = a$ and $-(a+b) = (-a)+(-b)$.

A *ring* is a set R with two operations: addition and multiplication such that

1. $(R, +)$ is an Abelian group;
2. $(R, \cdot)$ is a semigroup;
3. the *distributive law* holds on both sides: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ hold for any a, b and c.