Chapter 1

Groups

1.1 Monoids

Let S be a set. A mapping $f : S \times S \to S$ is called a law of composition. If $x, y \in S$, the evaluation $f(x, y)$ is called the product of x and y, and is denoted xy. If $x, y, z \in S$ are three different elements, we may form their product in two different ways, namely $(xy)z$ and $x(yz)$. If $x(yz) = (xy)z$, then the law of composition is **assosciative**, and the parantheses can be ommitted.

An element $e \in S$ is said to be an identity element if for all $x \in S$, $ex = xe = x$. An identity element is unique, since if $e, e' \in S$ are both identities, then $e = ee' = e'$.

Definition 1.1.1 *A set G, equipped with an assosciative law of composition, and an identity element, is called a **monoid***

Definition 1.1.2 *Given a monoid G, a **submonoid** $H \subset G$ is a subset containing the identity, and that is closed under the composition law of G. That is, if $x, y \in H$, then $xy, \in H$ as well.*

Example 1.1.1 *The set $\mathbb{N}$ of natural numbers form a monoid, where the law of composition is addition, with identity element* 0

1.2 Groups

Definition 1.2.1 *A **group** G is a monoid such that for every element $x \in G$, there is an element $y \in G$ such that $xy = yx = e$. The element y is called the **inverse** of x, denoted x^{-1}.*

An inverse of an element must be unique. To show this, suppose $y, y' \in G$ are both inverses of x. Then

$$y = ye = y(xy') = (yx)y' = ey' = y'$$

Example 1.2.1 *Let G be a group, S a non-empty set. Then the $M(S, G) = \{f : S \to G\}$ is a group, where if $f, g \in M(S, G)$, the product fg is defined as $(fg)(x) = f(x)g(x)$, and inverses such that $f^{-1}(x) = f(x)^{-1}$. Then $M(S, G)$ is a group. If G is abelian, then so is $M(S, G)$*

Example 1.2.2 *The set of rational numbers $\mathbb{Q}$ is a group under addition. The set of non-zero rationals $\mathbb{Q} \setminus \{0\}$ is a group under multiplication. Similar statements hold for the real numbers $\mathbb{R}$ and the complex numbers.*

Definition 1.2.2 *A group G is said to be **cyclic** if there is some element $a \in G$ such that for every $g \in G$, there is an integer n so that $g = a^n$*

Example 1.2.3 *The set of integers $\mathbb{Z}$ is cyclic, with generator 1, or alternatively, generator -1*

Example 1.2.4 *Fix a positive integer n. Then, the n-th roots of unity in the complex numbers form a cyclic group of order n. A generator for this group is a complex number of the form $\exp(2\pi ir/n)$, with $\gcd(r, n) = 1$*

Definition 1.2.3 *Let G_1, G_2 be groups. The **direct product** of G_1 and G_2, denoted $G_1 \times G_2$ is the set of all pairs (x_1, x_2), with $x_i \in G_i$. We define the law of composition componentwise - $(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2)$. The identity of this group is (e_1, e_2), where $e_i \in G_i$ is the identity of each respective group.*

The idea of a direct product of groups can be extended to the product of a family of n groups G_i, with $\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n$, with identity $(e_1, e_2, \ldots, e_n)$.

Definition 1.2.4 *Let G be a group. A* ***subgroup*** *H of G is a subset of G containing the identity element, and such that H is closed under the law of composition and taking inverses. A subgroup is* ***trivial*** *if it contains the identity element alone*

Definition 1.2.5 *Let G be a group, and S be a subset of G. Then S* ***generates*** *G, or S is the* ***set of generators*** *of G, if every element in G can be expressed as a product of elements of S or inverses of elements of S, that is a product $x_1 x_2 \cdots x_n$, where each x_i or x_i^{-1} is in S*

Clearly if S generates G, it is a subgroup of G. Furthermore, S is the smallest subgroup of G containing S. If G is generated by S, we write $G = \langle S \rangle$

Example 1.2.5 *There are two non-abelian groups of order 8. One is the* ***group of symmetries of the square****, generated by two elements σ, τ such that $\sigma^4 = \tau^2 = e$ and $\tau\sigma\tau^{-1} = \sigma^3$*
The other is the ***quaternion group****, generated by two elements i, j, such that if $k = ij$ and $m = i^2$, then $i^4 = j^4 = k^4 = e$, $i^2 = j^2 = k^2 = m$, and $ij = mji$*