Group Theory Notes

1 Revision of Groups

Definition 1.1.1: Definition of a Group

A **group** consists of a set G together with a function $G \times GztoG$ which maps an ordered pair $(g,h) \in G \times G$ to an element $g \star h \in G$. The following axioms must be satisfied:

1. **Associativity**: $(g \star h) \star k = g \star (h \star k)$ for each triple $(g,h,k) \in G \times G \times G$
2. **Identity**: $\exists e \in G$ such that $e \star g = g = g \star e$ for each $g \in G$
3. **Inverse**: To each element $g \in G$, there is an element $g^{-1} \in G$ such that $g \star h = e = h \star g$

Note: The closure axiom follows from the definition of a function.

Example 1.2.A: Examples of Groups

1.2.1) S_n, the n**-th symmetric group**, is the group of permutations of $\{1, 2, \ldots, n\}$, with composition of functions.

1.2.2) D_n, the n**-th dihedral group**, is the group of symmetries of the n-gon. It has $2n$ elements: n rotations, and n reflections.

1.2.3) The **free group** on the letters x, y is written as $G = \langle x, y \rangle$. The elements of G are **words** in the symbols x, y, x^{-1}, y^{-1}. The group operation $\star$ is **concatenation**: so $xxx^{-1}y \star y^{-1}x = xxx^{-1}yy^{-1}x$. e is the **empty word** with 0 letters, and x^{-1} and y^{-1} is the inverse of x and y respectively. Thus $xxx^{-1}y = xy$.

1.2.4) $(\mathbb{Z}, +)$ is a group, with $e = 0$. It is a **cyclic** group, and is **generated** by 1.

1.2.5) $\mathbb{Z}/n$, the set of integers modulo n, is a group under $+$.

Definition 1.2.6: Abelian Group

A group $(G, \star)$ is **abelian** if $g \star h = h \star g$ for all $g, h \in G$.
Note: Often, when $(G, \star)$ is ablian, we write $g + h$ as the group operation.

Definition 1.3.1: Subgroup

If H is a nonempty subset of G then H is a **subgroup** provided that:

- $hk \in H$ for all $h, k \in H$.
- $h^{-1} \in H$ for all $h \in H$.

We usually just say "H is closed under the group operations". Note that $e \in H$ follows from the definition, and associativity follows from the fact that G is a group. Any subgroup H of G is a group using the same product as that of G.
We write $H \leq G$ when H is a subgroup of G (as opposed to $H \subseteq G$ which just means H is a subset of G). The notation $H < G$ means that H is a subgroup of G and $H \neq G$. A subgroup H is **proper** if $H \neq G$ and is **non-trivial** if $H \neq \{e\}$.

Example 1.3.A: Examples of Subgroups

1.3.2) The subsets $\{e\}$ and G are always subgroups of G

1.3.3) The group of rotations of an n-gon is a subgroup of D_n

1.3.4) The n**-th alternating group**, A_n is the subgroup of S_n consisting of all permutations that can be written as the product of an even number of 2-cycles.

1.3.5) Let G be a group and $g \in G$. Then $\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$ is a subgroup of G, called the **subgroup generated by** g. If $G = \langle g \rangle$ for some $g \in G$, then G is **cyclic**.

Definition 1.3.6: Coset

Let $H \leq G$ and $g \in G$. Then the **left coset** of H determined by g is the set

$$gH := \{gh \mid h \in H\}$$

Similarly, the **right coset** of H determind by g is the set

$$Hg := \{hg \mid h \in H\}$$