653 Notes

0.1 Group Theory

Let S be a set. A **Product** on S is a function $S \times S \to S$, where $(s,t) \mapsto s \cdot t$. If $s \cdot t = t \cdot s$, we say $\cdot$ is **commutative** and write $s + t$. A product is **associative** if $(s \cdot t) \cdot u = s \cdot (t \cdot u)$. An element $e \in S$ is an **identity** if for all $s \in S$, we have $e \cdot s = s \cdot e = s$. Identities are unique. A **Monoid** is a set M equipped with an associative product that contains an identity.

Example. The set func(S) of functions on S is a monoid under function composition with identity $e : s \mapsto s$.

Example. The subsets of a set S form a monoid under intersection with identity X, as well as under set union with identity $\emptyset$.

If a monoid M has a commutative product, M is called an **abelian monoid**. A **submonoid** of a monoid M is a subset $H \subset M$ with $e \in H$ and $xy \in H$ for all $x, y \in H$.

Example. The set $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 0\}$ is a monoid under $+$ with identity 0, and under $\cdot$ with identity 1. The element 0 is called absorbing in this case.

Example. For all $a \in \mathbb{N}$, $a\mathbb{N}$ is a monoid under addition but not multiplication unless $a = 1$, since it does not contain 1.

A **Group** G is a monoid such that for every $x \in G$, there exists a $y \in G$ such that $xy = e$. In this case we write $y = x^{-1}$. Note that $xy = e$ implies that $yx = e$. In a group, both inverses and the identity are unique. In a group, equations $ax = b$ and $xa = b$ have unique solutions. A **Subgroup** of a group G is a submonoid of G that is closed under the action of taking inverse.

Example. $\{e\}$ is a trivial example of a group. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are all examples of groups under addition.

Example. $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$ is a group under multiplication, along with $\mathbb{R}^\times$ and $\mathbb{C}^\times$, defined in an analagous way.

Example. The unit complex numbers S^1 form a group under complex multiplication

Example. Let S be a set and define Sym(S) to be the set of bijections $S \to S$. Then Sym(S) is a group under composition called the **Symmetric Group** on S.

Let M, M' be monoids with identities e, e' respectively. A **homomorphism** of monoids is a function $f : M \to M'$ such that $f(e) = e'$, and for all $x, y \in M$, we have $f(xy) = f(x)f(y)$. A monoid homomorphism between groups is a group homomorphism.

We say a group is **cyclic** if there exists $a \in G$ such that any $g \in G$ can be written $g = a^n$ for some $n \in \mathbb{Z}$. When this occurs, we say a **generates** G.

Example. $\mathbb{Z}$ has two generators, 1 and -1.

Example. The nth roots of unity, denoted C_n, has generators $e^{2\pi \frac{k}{n}}$, where $\gcd(n,k) = 1$.

Let G and H be groups. We can define a product on $G \times H$ by $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$. Then $G \times H$ is a group with identity $e = (e_G, e_H)$ and with inverse $(g,h)^{-1} = (g^{-1}, h^{-1})$. This construction generalizes to arbitrary product with component-wise multiplication.

Let G be a group and $S \subset G$. We define $\langle S \rangle$, the subgroup **generated** by S to be the collection of all finite combinations of elements of S. Equivalently, $\langle S \rangle$ is the smallest subgroup of G containing S, or the intersection of all subgroups containing S. If $a \in G$, the order of a is the smallest $n > 0$ such that $a^n = e$. Equivalently the order of a is the number of elements in $\langle a \rangle$.