653 Notes

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 $\varnothing$.

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 $\langle a \rangle$.

Remark. Suppose $S \subset G$ and $G = \langle S \rangle$. Then any homomorphism $G \to H$ is determined by its restriction to S.

Not all functions $\varphi : S \to H$ give homomorhpisms.

Definition. An isomorphism $G \to G$ is called an automorphism. We denote $\mathrm{Aut}(G)$ the set of automorphisms of a group G.

dy

Example. For $m \in \mathbb{Z}$, $a \mapsto a \cdot m$ is a homomorphism $\mathbb{Z} \to \mathbb{Z}$. If $m \neq 0$, the map is an injective homomorphism, called a monomorphism.

Definition. We denote $\mathbb{Z}_m$ the set of integers mod m.

The map $a \mapsto a \mod m$ is a homomorphism $\mathbb{Z} \to \mathbb{Z}_m$.

Example. The exponential map is a homomorphism $(\mathbb{R}, +) \to (\mathbb{R}_>, \cdot)$. The inverse map is the logarithm.

Theorem 0.1. *Let f be a group homomorphism. Then $\ker f = \{e\}$ if an only if f is injective.*

Proposition 1 (Internal Direct Product)**.** *Let G be a group with subgroups H and K, such that $H \cap K = \{e\}$, and $H \cdot K = G$, and $hk = kh$ for all $h \in H, k \in K$. Then the map $\varphi : H \times K \to G$ given by $(h, k) \mapsto h \cdot k$ is an isomorphism.*

Proof. φ is surjective by $H \cdot K = G$. Homomorphism easy to check. To show injective, if $\varphi(h, k) = e$, then $hk = e$ and $k \in H$, therefore $k = e$. The same applies for $h = e$. Then $(h, k) = (e, e)$.

Cosets and Lagrange's Theorem

Definition. Let H be a subgroup of a group G. A left (right) coset of H in G is a subset of the form aH (Ha) for some $a \in G$.

Theorem 0.2. *Let H be a subgroup of a group G. Then*

- $aH = bH$ *iff* $b \in aH$ *iff* $aH \cap bH \neq \varnothing$ *iff* $b^{-1}a \in H$
- *for all $a \in G$, H and aH are in non-canonical bijection*
- *the relation $a \sim b$ if $aH = bH$ is an equivalence relation on G.*
- *the map $aH \mapsto Ha^{-1}$ is a bijection between left and right cosets of H.*

Definition. The index of a subgroup H of G, denoted $[G : H]$, is the cardinal number of the set of right cosets of H in G.

Theorem 0.3. *Let G be a group and H a subgroup. Then $|G| = [G : H] \cdot |H|$.*

Proof. The cosets of H partition G and are equinumerous with H.

Normal Subgroups

Definition. A subgroup N of G is called normal if for all $g \in G$, $gN = Ng$.

Theorem 0.4. *Let N be normal in G and let G/N be the set of cosets of N in G. Then G/N is a group with product $aN \cdot bN = abN$. We call G/N the quotient or factor group of G by N.*

Proof. Let $\alpha \in aN$ and $\beta \in bN$. Then there exist $m, n \in N$ such that $\alpha = an$ and $\beta = bm$. Then $\alpha \cdot \beta = anbm = ab(b^{-1}nb)m \in abN$.

One also must check for inverses and identity.

We call the map $G \to G/N$ sending $a \to aN$ the canonical surjection/map. N is the kernel of the canonical surjection.

Definition. A sequence

$$A \xrightarrow{f} G \xrightarrow{g} K$$

is called exact at G if $\ker g = \mathrm{im} f$.

If $N \trianglelefteq G$, then

$$0 \xrightarrow{i} N \xrightarrow{j} G \xrightarrow{\varphi} G/N \xrightarrow{f} 0$$

is exact everywhere.

Suppose

$$e \longrightarrow H \xrightarrow{f} G \xrightarrow{g} K \longrightarrow e$$

is exact. We call this a short exact sequence. Let $N = \mathrm{im} f$. Then we get a commutative diagram

$$\begin{tikzcd}
e \arrow[r] & H \arrow[r, "f"] \arrow[d, "f"] & G \arrow[r, "g"] \arrow[d] & K \arrow[r, "p"] \arrow[d, "\psi"] & e \\
e \arrow[r] & N \arrow[r, "i"] & G \arrow[r, "\varphi"] & G/N \arrow[r] & 0
\end{tikzcd}$$

where the vertical arrows are isomorphisms.

Proof. Let $k \in K$. There exists $a \in G$ such that $g(a) = k$ since $\mathrm{im}\, g = \ker p = K$. Then $\varphi(a) \in G/N$. Set $\psi(k) = \varphi(a)$. Suppose $g(b) = k$. Then $\varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) = e$, because $g(a) = g(b)$ implies $ab^{-1} \in \ker g = \mathrm{im}\, f = N = \ker \varphi$.