Group Theory Cheat Sheet

Group Axioms

A group is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G satisfying the following axioms:

- **Associativity:** $(a * b) * c = a * (b * c) \forall a, b, c \in G$
- **Identity:** $\exists e \in G$, called an identity element of G, s.t. $\forall a \in G$ we have $a * e = e * a = a$.
- **Inverse** $\forall a \in G \exists\ a^{-1} \in G$, called an inverse of a, s.t. $a * a^{-1} = a^{-1} * a = e$.

Closure is guaranteed due to the definition of binary operation.
Identity and inverses are unique.

Some Special Groups

- A group is called **abelian** if it is commutative.
- The group of all symmetries of a $n-$sided regular polygon is called the **dihedral group**. It is represented as,

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle.$$

- The group of all bijections on a set on n elements is called the **symmetric** group denoted as S_n.
- The **Klein-4** group is a group with 4 elements in which each element is a self inverse.

Homomorphisms and Isomorphisms

Let $(G, *)$ and $(H, \circ)$ be groups. A map $\varphi : G \to H$, $s.t.$ $\varphi(x * y) = \varphi(x) \circ \varphi(y)\ \forall\ x, y \in G$ is called a **homomorphism.**
A bijective homomorphism is called an **isomorphism**.

Subgroups

For a Group G a subset $H \subseteq G$, is a **subgroup** of G, i.e. $H \leq G$ if it is non empty and a group with the binary operation of G restricted to H.
Alternatively, a subset of a group is a subgroup if it is non empty and closed under products and inverses, i.e. for $H \subseteq G$

- $H \neq \emptyset$
- $xy^{-1} \in H, \forall x, y \in H$

A subgroup N of G is called **normal**, denoted as $N \trianglelefteq G$ if $gng^{-1} \in N, \forall\ g \in G, n \in N$.

Group Actions

A **group action** of a group $(G, *)$ on a set X is a map $\circ : G \times X \to X$ satisfying the following properties,

- **Identity:** $e \circ x = x, \forall x \in X$
- **Compatibility:** $g \circ (h \circ x) = g * h \circ x, \forall g, h \in G, x \in X$

Alternatively a group action on a set X can be thought of as a homomorphism from G to the symmetric group of X.
The **conjugation action** is a homomorphism $\varphi_x : G \to G$ for some fixed $x \in G$ is defined as $\varphi_x(g) = xgx^{-1}$.

Stablizer, Kernel of Group Action

If G acts on a set X then we define the following,
Orbit of a $x \in X$ is the set $Gx = \{gx \in X \mid g \in G\}$. Alternatively its the equivalence class induced by the group action.
Stablizer of an element $x \in X$ is the set of elements from the group which leave x fixed, i.e. $G_x = \{g \in G \mid gx = x\}$
Kernel of a group action is the kernel of the associated group homomorphism i.e., $\{g \in G \mid gx = x, \forall x \in X\}$
An action is called **transitive** if it has only one orbit, and is called **faithful** if its kernel is trivial.
Conjugacy classes of G is the equivalence classes of G when it acts on itself with conjugation. i.e. $\{gag^{-1} \mid g \in G\}$

Centralizers and Normalizers

Centralizer of $A \subseteq G$ in G is a subset of G defined as

$$C_G(A) = \{g \in G \mid gag^{-1} = a\ \forall\ a \in A\}.$$

It is the set of all elements of G which commute with every element of A.
Center of G is the subset of G defined as

$$Z(G) = \{g \in G \mid gx = xg\ \forall\ x \in G\}.$$

It is the set of elements commutating with all the elements of G. It is the kernel of the conjugation action.
Normalizer of A in G is defined as

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}$$

$gAg^{-1} = \{gag^{-1} \mid a \in A\}$. Note that $C_G(A) \leq N_G(A)$. The normalizer of a subset is its stabilizer under conjugation action.

Cyclic Groups and Cycle Notation

A Group H is **cyclic** if $\exists\ x \in H$ s.t. $H = \{x^n \mid n \in \mathbb{Z}\}$
For the above case we say $H = \langle x \rangle$ and that H is generated by x.

- A cyclic group can have more than one generator.
- All cyclic groups are abelian.
- If $H = \langle x \rangle$ then $|H| = |x|$, if $|H| = n < \infty$ then $x^n = 1$
- Any two cyclic groups of the same order are isomorphic.

Two-Line to Cycle notation for permutations
$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} = (125)(34) = (34)(125) = (34)(512) = (15)(25)(34)$
Here, the last form is a case of 2-cycle (transposition).

Parity of Permutations and Alternating Groups

The parity of any permutation σ is given by the parity of the number of its 2-cycles (transpositions).

Alternating Groups:
An alternating group is the group of even permutations of a finite set of length n. It is denoted by A_n it's order is $\frac{n!}{2}$

Cosets and Quotient Groups

For any $N \leq G$ and any $g \in G$

- $gN = \{gn \mid n \in N\} = \{g, gh_1, gh_2 \dots\}$ and,
- $Ng = \{ng \mid n \in N\} = \{g, h_1 g, h_2 g \dots\}$ are called a left coset and a right coset respectively.

For a Group G and $N \trianglelefteq G$, the **quotient group** of N in G (i.e. G/N), is the set of cosets of N in G.
The definition of a normal subgroup is the same as left and right cosets being equal.

Lagrange's Theorem and some results

Lagrange's Theorem: For a finite group G and $H \leq G$,

- The order of H divides the order of G, and,
- The number of left cosets of H in G equals $\frac{|G|}{|H|}$

Some important results

- If G is a finite group and $x \in G$, then the order of x divides the order of G, and $x^{|G|} = e\ \forall\ x \in G$
- If G is a group of prime order, then G is cyclic

Cauchy's Theorem

Cauchy's Theorem: If G is a finite group and p is a prime dividing $|G|$ then G has an element of order p.

The Isomorphism Theorems

First Isomorphism Theorem:
If $\varphi : G \to H$ is a homomorphism of groups. Then $\ker\varphi \trianglelefteq G$ and, $G/\ker\varphi \cong \varphi(G)$.
Second Isomorphism Theorem:
For a group G with, $A, B \leq G$ and, $A \trianglelefteq N_G(B)$. Then $AB \leq G$, $B \trianglelefteq AB, A \cap B \trianglelefteq A$ and, $AB/B \cong A/A \cap B$
The Third Isomoprhism Theorem:
For a group G with, $H, K \trianglelefteq G$ and, $H \leq K$. Then $K/H \trianglelefteq G/H$ and, $\frac{G/H}{K/H} \cong G/K$

Class equations and Orbit-stabilizer Theorem

Class equation of a finite group G is written as:
$|G| = |Z(G)| + |\sum(\text{Conjugancy classes of G})|$
Oribit-stabilizer Theorem:
For a group G acting on a set X, for any $x \in X$ we have, $|Gx||G_x| = |G|$

Cayley's Theorem

Cayley's Theorem:
Every group is isomorphic to a subgroup of some symmetric group. If G is a group of order n, then G is isomoprhic to a subgroup of S_n

Automorphisms

Automorphism of G is defined as an isomorphism from G onto itself.
The set of all automorphisms of G is denoted by $\text{Aut}(G)$

p-groups and Sylow p-groups

- **p-group** is defined as a group of order p^a for some $a \geq 1$. Sub-groups of G which are p-groups are called p-subgroups.
- **Sylow p-group** is defined as a group of order $p^a m$, where $p \nmid m$, a subgroup of order p^a is called a Sylow p-subgroup of G. $Syl_p(G)$ is the set of Sylow p-subgroups of G.

The Sylow Theorems

First Sylow Theorem:
If p divides $|G|$, then G has a Sylow p-subgroup.
Second Sylow Theorem:
All Sylow p-subgroups of G are conjugate to each other for a fixed p.
Third Sylow Theorem:
$n_p \equiv 1 (\text{mod } p)$, where n_p is the number of Sylow p-subgroups of G.

Commutators

For a group G and $x, y \in G$ call $[x, y] = x^{-1}y^{-1}xy$ the **commutator** of x and y.
For subsets $A, B \subseteq G$ define the group generated by its commutators as $[A, B] = \langle [a, b] \mid a \in A, b \in B \rangle$.
Similarly $G' = [G, G]$ is the subgroup of G generated by all commutators, its called the commutator subgroup of G, or its **derived subgroup**.
The following are some useful properties of commutators,

- $xy = yx \iff [x, y] = 1$
- $H \trianglelefteq G \iff [H, G] \leq H$
- G/G' is abelian and its the largest abelian quotient of G. It is called the **abelianization** of G.
- Any homomorphism from G to an abelian group A factors through G'. i.e. its universal

Direct products

The **direct product** $G_1 \times G_2 \times \cdots$ of groups $G_1, G_2, \ldots$ is set of sequences $(g_1, g_2, \cdots)$ with $g_i \in G_i$ and operation $*$ defined component wise.
If H, K are normal subgroups of G with $H \cap K = 1$ then $HK \cong H \times K$

Semidirect products

Let H, K be groups and φ be a homomorphism from $K \to \text{Aut}(H)$. The semidirect product of H and K with respect to φ denoted as $H \rtimes_\varphi H$ is defined as an ordered pair $(h, k), h \in H, k \in K$ with multiplication defined as $(h_1, k_1)(h_2, k_2) = (h_1 k_1 h_2, k_1 k_2)$.

Fundamental theorem of finite abelian groups

Every finite abelian group can be written as a direct product of cyclic groups of prime power order.

Schur-Zassenhaus Theorem

If G is a finite group and $N \trianglelefteq G$ and $(|G|, |G/N|) = 1$ then $G = N \rtimes G/N$

Simple groups and Composition Series

A group G is called **simple** if $|G| > 1$ and its only normal subgroups are 1 and G.
A sequence of subgroups as follows (called a subnormal sequence),

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{k-1} \leq N_k = G$$

is called a **composition series** if N_{i+1}/N_i is simple, for $i = 0, \ldots k-1$. The quotient groups are called composition factors.

Jordan Hölder theorem

Every finite non trivial group G has a composition series and the composition factors are unique up to permutation.

Solvable groups

A group G is called **solvable** if there is a chain of normal subgroups with each subsequent quotient group being abelian.
Alternatively if there exists $G^{(n)} = 1$ for some $n \geq 0$ where we define the **commutator/derived series** as follows,

$$G^{(0)} = G, G^{(1)} = [G, G], \text{ and } G^{(i+1)} = [G^{(i)}, G^{(i)}]$$

- If $N \trianglelefteq G$ and $N, G/N$ are solvable then G is solvable.
- Burnsides theorem: If $|G| = p^a q^b$ for primes p, q then G is solvable
- Feit-Thompson: All finite groups of odd order are solvable.

Nilpotent groups

A group is called **nilpotent** if its **lower central series** defined below terminates,

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = 1, G_{i+1} = [G_i, G].$$

and n is called its nilpotency class.