Intro 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:
i. Closure: ∀ a, b ∈ G, a * b, is also in G
ii. Associativity: (a * b) * c = a * (b * c), ∀ a, b, c ∈ G
iii. Identity: ∃ e ∈ G, called an identity of G,
s.t. ∀ a ∈ G we have a * e = e * a = a
iv. Inverse ∀ a ∈ G ∃ a^{-1} ∈ G, called an inverse of a, s.t. a * a^{-1} = a^{-1} * a = e.

Some Properties of Groups

i. Abelian group A group G is abelian if a * b = b * a ∀ a, b ∈ G
ii. Finite group A group G is finite if the number of elements in G are finite
iii. Cancellation property suppose that a * b = a * c, ∀ a, b, c ∈ G, ⇒ b = c
iv. Uniqueness of Inverse and Identity
- The identity of G is unique
- ∀ a ∈ G, a^{-1} is uniquely determined
- $(a^{-1})^{-1}$ = a ∀ a ∈ G
- $(a * b)^{-1} = (b^{-1}) * (a^{-1})$
- for any $a_1, a_2, ..., a_n$ ∈ G the value of $a_1 * a_2 *$ ůůů $* a_n$ is independent of how the expression is bracketed

Some Special Groups

i. Dihedral Group (D_n or D_{2n}) is a group of symmetries of a n-sided regular polygon. Order = 2n
ii. Symmetric Group (S_n) is the group whose elements are all the bijections from the set to itself.
Order = n!
iii. Klein-4 Group (K_4 or V) is a group with 4 elements in which each element is a self inverse.

Homomorphisms and Isomorphisms

i. Homomorphisms
Let (G , *) and (H, ∘) 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.**
ii. Isomorphism
For φ : G → H is called an **isomorphism** if:
i. φ is a homomorphism
ii. φ is a bijection

Group Actions

A **group action** of a group G on a set A is a map from G × A to A satisfying the following properties
i. Identity: $e \cdot x = x$ and,
ii. Compatibility: $g \cdot (h \cdot x) = (gh) \cdot x$

Subgroups

For a Group G. The subset H of G, is a **Subgroup** of G, i.e. H ≤ G if
i. H is non-empty
ii. H is closed under products and inverses
- **A Normal subgroup** N of G, (i.e. $N \trianglelefteq G$) iff $gng^{-1} \in N\ \forall\, g \in G$ and $n \in N$.

The Subgroup Criterion
A subset H of group G is a subgroup of G iff
i. H ≠ ∅
ii. $\forall\, x,\ y \in H\ xy^{-1} \in H$

Centralizers, Normalizers, Stabilizers and Kernels

- **Centralizer** of A 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. Note, this is case $Z(G) = C_G(G)$ so $Z(G) \leq G$.
- **Normalizer** of A in G is defined as the set
$N_G(A) = \{g \in G \mid gAg^{-1} = A\}$ where,
$gAg^{-1} = \{gag^{-1} \mid a \in A\}$. Note that $C_G(A) \leq N_G(A)$.
- **Stabilizer** on a set S with element s in G is defined as the set
$G_s = \{g \in G \mid g \cdot s = s\}$. Note that $G_S \leq G$.
- **Kernel** of G on S is defined as the set
$Ker(f) = \{g \in G \mid g \cdot s = s\ \forall\, s \in S\}$

Cyclic Groups and Cycle Notation

A Group H is **Cyclic** if $\exists\, x \in H$ s.t. $H = \{x^n \mid n \in \boldsymbol{Z}\}$
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).

Cosets and Quotient Groups

For any $N \leq G$ and any $g \in G$
- $gN = \{gn \mid n \in N\} = \{g, gh_1, gh_2 \ldots\}$ and,
- $Ng = \{ng \mid n \in N\} = \{g, h_1g, h_2g \ldots\}$ 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.

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

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

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 $\frac{n!}{2}$

Equivalence Classes and Orbits

- If G is a group acting on the non-empty set A. Then $a \sim b \iff a = g \cdot b$ for some $g \in G$. Where $\sim$ is an equivalence relation.
- The **orbit** of G containing a is given as $\mathcal{O}_a = \{g \cdot a \mid g \in G\}$
- The action of G on A is called transitive if there is only one orbit.
- **Conjugacy classes** of G is the equivalence classes of G when it acts on itself with conjugation. i.e. $\{gag^{-1} \mid g \in G\}$

Class equations and Orbit-stabilizer Theorem

Class equation of a finite group G is written as:
$|G| = |Z(G)| + |\sum$(Conjugancy classes of G)$|$
Oribit-stabilizer Theorem:
For a group G acting on a set S, for any $s \in S$ we have, $|\mathcal{O}_s||G_s| = |G|$

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 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

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