Algebra I Reference Sheet

Groups

(Def.) A set G with operation $\circ$ is a **Group** under $\circ$ if

1. G is closed under $\circ$ (Binary Operation)
2. G has an identity.
3. G has inverses.
4. G is associative.

Terminology

1. Dihedral Group, $D_n, n \geq 3$ (Order $2n$)
2. Abelian (Commutative)
3. Cayley Table
4. $GL(n, F), SL(n, F), \mathbb{Z}_n, U(n)$, $n \in \mathbb{N}$
5. Shoe-Socks Property, $(ab)^{-1} = b^{-1}a^{-1}$

Subgroups

(Def.) A subset of a Group is a **Subgroup** if it is itself, a group under the same operation.

3-Step Subgroup Test

$S \leq G$ (Subgroup notation) iff

1. $S \neq \varnothing$
2. S is closed under $\circ$
3. S has inverses. ($a \in S \Rightarrow a^{-1} \in S$)

Terminology

1. Proper Subgroup
2. Order of a Group & Order of element
3. Center of a Group
4. Centralizer of an element

Cyclic Groups

A group, G, is **Cyclic** if $\exists g \in G$ such that $G = \{g^n : n \in \mathbb{Z}\} = \langle g \rangle$. We say g a generator of G.

Properties

1. For a in a group of order n, $a^i = a^j$ iff $n | i - j$
   (a) If the group is infinite, $a^i = a^j$ iff $i = j$ and $a \neq e$
2. For a in a group of order n, $\left\langle a^k \right\rangle = \left\langle a^{gcd(n,k)} \right\rangle$ and $|a^k| = n/gcd(n, k)$ for $k \in \mathbb{Z}^+$
3. Every subgroup of a cyclic group is cyclic.
4. Say $G = \langle a \rangle, a \in G, |a| = n$. Then $\langle a \rangle = \left\langle a^k \right\rangle$ iff $gcd(n, k) = 1$.

Terminology

1. Subgroup Lattice

Permutations

(Def.) A **Permutation** of a set A is a bijection from $A \to A$. A **Permutation Group** is a set of permutations that form a group under function composition.

Properties

1. Every permutation of a finite set can be written as the product of disjoint cycles.
2. Disjoint cycles are commutative.
3. The order of a permutation is the LCM of the lengths of its disjoint cycles.
4. Every permutation in S_n, $n > 1$, is a product of 2-cycles.

Terminology

1. Cycle Notation
2. Symmetric Group of degree n, S_n is the group of all permutations on $\{1, 2, \ldots, n\}$
3. Even/Odd Permutations (# of 2-cycles)
4. Alternating Group of degree n, A_n, is the set of even permutations in S_n.

Isomorphisms

(Def.) An **Isomorphism**, ϕ from a group G to a group $\overline{G}$ is a bijection that preserves operations, that is

$$\phi(ab) = \phi(a)\phi(b) \quad \forall\, a, b \in G$$

If an isomorphism exists from $G \to \overline{G}$ then we say that G and $\overline{G}$ are **Isomorphic** and write $G \approx \overline{G}$.

Cayley's Theorem

Every group is isomorphic to a group of permutations, T with

$$T = \{T_g : g \in G\} \text{ where } T_g(x) = gx \,\forall x \in G$$

Properties

Let $\phi : G \to \overline{G}$ be an isomorphism.

1. $\phi(e) = \overline{e}$, $e \in G, \overline{e} \in \overline{G}$.
2. For $a \in G$, $\phi(a^n) = [\phi(a)]^n$
3. For $a, b \in G$, $ab = ba$ iff $\phi(a)\phi(b) = \phi(b)\phi(a)$.
4. G is Abelian iff $\overline{G}$ is Abelian.
5. $G = \langle a \rangle$ iff $\overline{G} = \langle \phi(a) \rangle$.
6. $|a| = |\phi(a)|$ (Isomorphisms preserve order)
7. G is cyclic iff $\overline{G}$ is cyclic.
8. ϕ^{-1} is an isomorphism.
9. If $H \leq G$, then $\phi(H) = \{\phi(h) : h \in H\} \leq \overline{G}$.
10. $Aut(\mathbb{Z}_n) \approx U(n)$

Terminology

1. Automorphism (Isomorphism from $G \to G$)
2. Inner Automorphism (induced by a), ϕ_a, $a \in G$ such that $\phi_a(x) = axa^{-1}, \forall x \in G$.
3. $Aut(G), Inn(G)$ the group of automorphisms and inner automorphisms on G.

Cosets

(Def.) Let G be a group and $H \leq G$. Then the **Left Coset** of H in G containing a is $aH = \{ah : h \in H\}$. **Right Cosets** are similar.

Properties

Let $(G, \circ)$ be a group, $H \leq G, a \in G$. All properties apply to right cosets similarly.

1. $a \in aH$ (since $ae \in aH$)
2. $aH = H$ iff $a \in H$.
3. Distinct left cosets are disjoint.
4. $aH = bH$ iff $a^{-1}b \in H$
5. $|aH| = |bH| = |H| \; \forall a, b \in G$
6. $aH = Ha$ iff $a^{-1}Ha = H$.
7. $aH \leq G$ iff $a \in H$ (so $aH = H$)
8. $G = \bigcup_{a \in G} aH$

Lagrange's Theorem

If G is a finite group and $H \leq G$. Then $|H|$ divides $|G|$. Moreover the number of distinct left cosets is $|G|/|H|$.

External Direct Products

(Def.) Let $G_1, G_2, \ldots, G_n$ be groups. Then the **external direct product** of $G_1, G_2, \ldots, G_n$ is

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_1, g_2, \ldots, g_n) : g_i \in G_i\}$$

Note: The product of elements is done component-wise, so we use the operation of each G_i for its components.

Properties

1. $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ is a group.
2. $|G_1 \oplus G_2 \oplus \cdots \oplus G_n| = |G_1||G_2| \cdots |G_n|$
3. $|(g_1, g_2, \ldots, g_n)| = lcm(|g_1|, |g_2|, \ldots, |g_n|)$
4. Let G, H be finite groups. $G \oplus H$ is cyclic iff $|G|, |H|$ are coprime.
5. If G is finite Abelian, then
   $$G \approx \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{k_n}}$$
   for primes p_i, and $k_i \in \mathbb{N}$.

Normal Subgroups

(Def.) A subgroup H of a group G is called a **normal subgroup** of G if $aH = Ha \; \forall a \in G$, denoted $H \triangleleft G$.

Normal Subgroup Test

$H \triangleleft G$ iff $xHx^{-1} \subseteq H \; \forall x \in G$.

Factor Groups

(Def.) Let G be a group and $H \triangleleft G$. The set

$$G/H = \{aH : a \in G\}$$

is a group under the operation $(aH)(bH) = (ab)H$.

Terminology

1. Internal Direct Product. $G = H \times K$ iff H, K are normal subgroups of G and
   $$G = HK = \{hk : h \in H, k \in K\}$$
   and $H \cap K = \{e\}$

Group Homomorphisms

(Def.) Given groups $G, \overline{G}$ and function $\phi : G \to \overline{G}$, then ϕ is a **group homomorphism** if ϕ preserves operations.

Kernel of ϕ

(Def.) $Ker(\phi) = \{g \in G : \phi(g) = \overline{e}\}$

Properties

Given group homomorphism $\phi : G \to \overline{G}$, $g \in G$, $H \leq G, \overline{K} \leq \overline{G}$.

1. $\phi(e) = \overline{e}$
2. $n \in \mathbb{Z}, \phi(g^n) = [\phi(g)]^n$
3. If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$
4. $Ker(\phi) \leq G$
5. $\phi(G) \leq \overline{G}$
6. The inverse image of $\overline{K}$,
   $$\phi^{-1}(\overline{K}) = \{k \in G : \phi(k) \in \overline{K}\}$$
   is a subgroup of G.
7. If H is cyclic, then $\phi(H)$ is cyclic.
8. If H is Abelian, then $\phi(H)$ is Abelian.
9. If $H \triangleleft G$, then $\phi(H) \triangleleft \phi(G)$.
10. If $\overline{K} \triangleleft \overline{G}$, then $\phi^{-1}(\overline{K}) \triangleleft G$.
11. If ϕ is a bijection, then ϕ is an isomorphism, then $G \approx \overline{G}$.

First Isomorphism Theorem

Given $\phi : G \to \overline{G}$ is a group homomorphism. Then

$$G/Ker(\phi) \approx \phi(G)$$
