Group Theory Quick Sheet

1. Groups

Definition 1 (Group)**.** A *group* $(G, \cdot)$ is a set with a binary operation such that for all $a, b, c \in G$: (1) $(ab)c = a(bc)$; (2) there exists $e \in G$ with $ea = ae = a$; (3) for each a there exists a^{-1} with $aa^{-1} = a^{-1}a = e$. If $ab = ba$ for all a, b, G is *abelian*.

Lemma 2 (Uniqueness of identity)**.** *A group has a unique identity element.*

Proof. □

Lemma 3 (Uniqueness of inverses)**.** *Each element of a group has a unique inverse.*

Proof. □

Lemma 4 (Inverse of a product)**.** *For all $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.*

Proof. □

Definition 5 (Order of an element)**.** The *order* of $a \in G$ is the least $m \geq 1$ such that $a^m = e$ (if it exists); otherwise the order is ∞.

Definition 6 (Cyclic groups)**.** A group G is *cyclic* if $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ for some $g \in G$.

2. Subgroups and Homomorphisms

Definition 7 (Subgroup)**.** A nonempty subset $H \subseteq G$ is a *subgroup* (written $H \leq G$) if for all $a, b \in H$, $ab^{-1} \in H$.

Definition 8 (Normal subgroup)**.** A subgroup $N \leq G$ is *normal* (written $N \trianglelefteq G$) if $gNg^{-1} = N$ for all $g \in G$.

Definition 9 (Homomorphism)**.** A map $\varphi : G \to H$ is a *homomorphism* if $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$.

Proposition 10 (Kernel and image)**.** *For a homomorphism $\varphi : G \to H$, the kernel* $\operatorname{Ker}\varphi = \{g \in G : \varphi(g) = e_H\}$ *and the image* $\operatorname{Im}\varphi = \varphi(G)$ *are subgroups; moreover* $\operatorname{Ker}\varphi \trianglelefteq G$.

Proof. □

Proposition 11 (Injectivity criterion)**.** *A homomorphism $\varphi : G \to H$ is injective if and only if* $\operatorname{Ker}\varphi = \{e\}$.

Proof. □

Definition 12 (Cosets and index)**.** For $H \leq G$ and $g \in G$, the *left coset* is $gH = \{gh : h \in H\}$. The *index* $[G : H]$ is the number of left cosets.

Theorem 13 (Lagrange's Theorem)**.** *If G is finite and $H \leq G$, then $|H|$ divides $|G|$ and $[G : H] = |G|/|H|$.*

Proof. □

Corollary 14 (Order divides group order)**.** *If G is finite and $a \in G$, then* $\operatorname{ord}(a) \mid |G|$.

Proof. $\square$

Definition 15 (Quotient group)**.** If $N \trianglelefteq G$, the set of cosets G/N is a group with $(gN)(hN) = (gh)N$.

3. Isomorphism Theorems

Theorem 16 (First Isomorphism Theorem)**.** *For a homomorphism $\varphi : G \to H$, there is a natural isomorphism $G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.*

Proof. $\square$

Theorem 17 (Second Isomorphism Theorem)**.** *If $A \leq G$ and $N \trianglelefteq G$, then $A \cap N \trianglelefteq A$, $AN \leq G$, and $A/(A \cap N) \cong AN/N$.*

Proof. $\square$

Theorem 18 (Third Isomorphism Theorem)**.** *If $N \trianglelefteq G$ and $K \trianglelefteq G$ with $N \subseteq K$, then $K/N \trianglelefteq G/N$ and $(G/N)/(K/N) \cong G/K$.*

Proof. $\square$

4. Group Actions

Definition 19 (Group action)**.** An action of G on a set X is a map $G \times X \to X$, $(g, x) \mapsto g \cdot x$, such that $e \cdot x = x$ and $g \cdot (h \cdot x) = (gh) \cdot x$.

Definition 20 (Orbit and stabilizer)**.** For $x \in X$, the *orbit* is $\operatorname{Orb}(x) = \{g \cdot x : g \in G\}$ and the *stabilizer* is $\operatorname{Stab}(x) = \{g \in G : g \cdot x = x\}$.

Theorem 21 (Orbit–Stabilizer)**.** *If G is finite and acts on X, then $|\operatorname{Orb}(x)| = [G : \operatorname{Stab}(x)]$ and $|\operatorname{Orb}(x)|\,|\operatorname{Stab}(x)| = |G|$.*

Proof. $\square$

Theorem 22 (Class equation)**.** *For the conjugation action of G on itself,*

$$|G| = |Z(G)| + \sum [G : C_G(g_i)],$$

where $Z(G)$ is the center, $C_G(g)$ the centralizer, and the sum runs over representatives of noncentral conjugacy classes.

Proof. $\square$

Remark 23 (Burnside's lemma (Cauchy–Frobenius)). For a finite action $G \curvearrowright X$, the number of orbits is

$$\#(X/G) = \frac{1}{|G|} \sum_{g \in G} \bigl|\{x \in X : g \cdot x = x\}\bigr|.$$

5. Sylow Theory

Definition 24 (Sylow p-subgroup)**.** Let $|G| = p^n m$ with $p \nmid m$. A *Sylow p-subgroup* is a subgroup of order p^n. The set $\mathrm{Syl}_p(G)$ has size $n_p = |\mathrm{Syl}_p(G)|$.

Theorem 25 (Sylow existence)**.** *If $|G| = p^n m$ with $p \nmid m$, then G has a subgroup of order p^n.*

Proof. ∎

Theorem 26 (Sylow conjugacy)**.** *Any two Sylow p-subgroups of G are conjugate.*

Proof. ∎

Theorem 27 (Sylow counting)**.** *The number n_p of Sylow p-subgroups satisfies $n_p \equiv 1 \pmod{p}$ and $n_p \mid m$.*

Proof. ∎

Theorem 28 (Cauchy's Theorem)**.** *If a prime p divides $|G|$, then G contains an element of order p.*

Proof. ∎

Corollary 29 (Normal Sylow criterion)**.** *If $n_p = 1$, then the unique Sylow p-subgroup is normal in G.*

Proof. ∎

6. Miscellaneous Facts

Theorem 30 (Subgroups of cyclic groups)**.** *Every subgroup of a cyclic group is cyclic.*

Proof. ∎

Theorem 31 (Subgroups by divisors)**.** *If G is cyclic of order n, then for each $d \mid n$ there is a unique subgroup of order d.*

Proof. ∎

Proposition 32 (Normalizer test for normality)**.** *A subgroup $N \leq G$ is normal if and only if $gNg^{-1} = N$ for all $g \in G$.*

Proof. ∎

Proposition 33 (Centralizer index and class size)**.** *For $x \in G$, the size of the conjugacy class of x equals $[G : C_G(x)]$.*

Proof. ∎

Proposition 34 (Coprime orders multiply in abelian groups)**.** *If G is abelian and $a, b \in G$ have coprime finite orders, then $\mathrm{ord}(ab) = \mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b)) = \mathrm{ord}(a)\,\mathrm{ord}(b)$.*

Proof. ∎

Remark 35 (Handy notation)*.* $Z(G)$ center, $C_G(x)$ centralizer, $N_G(H)$ normalizer, $\mathrm{Aut}(G)$ automorphism group, $\mathrm{Inn}(G)$ inner automorphisms.