Math 460 Fall 2025 - Class Notes

Joshua Gonzalez

1 Partitions and Equivalence Relations

Definition 1.1 (Partition). Given a set S, a partition of S is a collection \mathcal{P} of subsets of S such that:

- 1. Every $P \in \mathcal{P}$ is nonempty.
- 2. Every $s \in S$ belongs to exactly one $P \in \mathcal{P}$.

Remark 1.1. Given a set S, a binary relation \sim on S is a subset of $S \times S$. Usually, for $a, b \in S$, we write $a \sim b$ iff (a, b) lies in the subset.

Definition 1.2 (Equivalence Relation). A binary relation \sim on a set S is an equivalence relation if it is:

- 1. Reflexive: for every $x \in S$, $x \sim x$
- 2. Symmetric: for every $x, y \in S$, if $x \sim y$, $y \sim x$.
- 3. Transitive: for every $x, y, z \in S$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

Remark 1.2. If \sim is an equivalence relation on S, then for any $t \in S$, the equivalence class of t is defined as $C_t = \{s \in S : s \sim t\}$. The set of all equivalence classes forms a partition of S.

Remark 1.3. Giving a partition on S corresponds to giving an equivalence relation on S.

2 Functions

Remark 2.1. Suppose A and B are sets.

- 1. The identity function on A is the function $id_A: A \to A$ defined by $id_A(x) = x$
- 2. Given a function $f: A \to B$ and subsets $S \subseteq A$ and $T \subseteq B$, the image of S under f is defined as $f(S) = \{f(x) : x \in S\} \subseteq B$.
- 3. The inverse image (or preimage) of a subset $T \subseteq B$ under f is defined as $f^{-1}(T) = \{y \in A : f(y) \in T\} \subseteq A$.

Definition 2.1 (Injective, Surjective, Bijective). Let $f: A \to B$ where A and B are sets.

- 1. f is injective (or 1-1) if, whenever f(x) = f(y) for $x, y \in A$, then x = y.
- 2. f is surjective (or onto) if, for every $y \in B$, there exists $x \in A$ such that f(x) = y.
- 3. f is bijective if it is both injective and surjective.

3 Groups

Definition 3.1 (Group). A group is a pair (G, \cdot) where G is a set and \cdot is a binary operation on G, satisfying:

- 1. (Associativity) for all $a, b, c \in G$, (ab)c = a(bc)
- 2. (Identity) There exists an identity element 1_G s.t. for all $a \in G$, $a1_G = 1_G a = a$.
- 3. (Inverses) For every $a \in G$, there exists $a^{-1} \in G$ such that $aa^{-1} = 1_G = a^{-1}a$.

Remark 3.1. A binary operation on a set G is a function from $G \times G$ to G defined as $(a,b) \mapsto a \cdot b = ab$.

Remark 3.2 (Uniqueness of Identity and Inverses).

- 1. The identity element 1_G is unique.
- 2. The inverse a^{-1} of any element $a \in G$ is unique.

Definition 3.2 (Abelian Group). A group G is called abelian (or commutative) if ab = ba for all $a, b \in G$.

Definition 3.3 (Subgroup). A subgroup of a group (G, \cdot) is a subset H of G s.t. (H, \cdot) is a group. We write $H \leq G$ to denote "H is a subgroup of G". Where \cdot is the binary operation from G and H is closed under the group op in G, i.e. "H is closed under \cdot ".

Remark 3.3. For any subgroup H of G, $1_H = 1_G$

Definition 3.4 (Subgroup Criterion). Suppose (G, \cdot) is a group and H is a nonempty subset of G. Then $H \leq G$ if and only if

- 1. for all $a, b \in H$, $ab \in H$ (closed under ·).
- 2. for all $a \in H$, $a^{-1} \in H$ (closed under taking inverses).

Lemma 3.1 (Finite Subgroup Criterion). Suppose (G, \cdot) is a group and H is a finite subset of G. Then $H \leq G$ if and only if $H \neq \emptyset$ and for all $a, b \in H$, $ab \in H$ (i.e. H is closed under \cdot).

Remark 3.4. Suppose G is a group, and S, T are subsets of G while $g \in G$. Then

- 1. $gS = \{gs : s \in S\}$
- $2. Sg = \{sg : s \in S\}$
- 3. $ST = \{st : s \in S, t \in T\}$

Definition 3.5 (Cosets). When $H \leq G$, a left coset (resp. right coset) of H in G is a set of the form gH (resp. Hg) for some $g \in G$.

Lemma 3.2. Any two left cosets of H in G have the same cardinality. (The same holds for right cosets.)

Definition 3.6 (Left and Right Cosets). When H is a subgroup of a group G

- 1. $G/H := \{gH : g \in G\}$ the set of all left cosets of H
- 2. $G \setminus H := \{ Hg : g \in G \}$ the set of all right cosets of H

Proposition 3.1. G/H is a partition of G. Similarly, $G\backslash H$ is a partition of G.

Theorem 3.1 (Lagrange's Theorem). Suppose G is a finite group and $H \leq G$. Then |H| divides |G|.

Remark 3.5. The converse of Lagrange's theorem is not true. The theorem does hold for cyclic groups.

Remark 3.6. For any set S we often write |S| to denote the cardinality of S. If S is finite, then |S| is a nonnegative integer. When S is a subgroup of a group, we also use o(S) to denote its cardinality.

Definition 3.7 (Index). We define the index of a subgroup H in G, denoted $[G:H]:=|G/H|=|G\backslash H|$ equals the number of distinct (left or right) cosets.

Definition 3.8 (Order of an Element). Let G be a group and $g \in G$. If $g^k = 1_G$ for some positive integer k, then the least such k is called the order of g denoted as o(g) or |g|. If $g^k \neq 1_G$ for every positive k, then we say g has infinite order and write $o(g) = \infty$.

Remark 3.7. If $g \in G$ has infinite order, then all the integer powers of g are distinct.

Proposition 3.2. Suppose G is a group and $g \in G$.

- 1. if $o(g) = \infty$, then $g^i = g^j$ if and only if i = j.
- 2. if $o(q) = n < \infty$, then $q^i = q^j$ if and only if n|(i-j).

Proposition 3.3. If G is a finite group, then for any $g \in G$, o(g) divides |G|.

Definition 3.9 (Normal Subgroup). Given a group G, a subgroup H of G. We say H is a normal subgroup of G if gH = Hg for all $g \in G$ and write $H \subseteq G$ if the following holds: $\forall k \in H, \forall g \in G, ghg^{-1} \in H$ the term ghg^{-1} is called a conjugate of h.

Proposition 3.4 (Equivalent definitions of Normal Subgroups). In particular, if $H \leq G$, then $H \subseteq G$ if and only if any of the following equivalent conditions hold:

- 1. gH = Hg for all $g \in G$.
- 2. aHbH = abH for all $a, b \in G$.
- (1) implies the coset spaces G/H and $G\backslash H$ coincide (equal as sets) (2) means we can define a binary operation on $G/H \times G/H \to G/H$ by $(aH, bH) \mapsto (ab)H = (aH)(bH)$ this map makes G/H into a group called the quotient group of G by H provided $H \leq G$.

Remark 3.8. Any subgroup of an abelian group is normal.

4 Group Homomorphisms

Definition 4.1 (Group Homomorphism). Suppose G and H are groups. A group homomorphism from G to H is a function $\varphi : G \to H$ such that $\forall a, b \in G, \varphi(ab) = \varphi(a)\varphi(b)$.

Remark 4.1 (Simple Facts). *if* $\varphi : G \to H$ *is a group homomorphism, then for any* $a \in G$,

- 1. $\varphi(1_G) = 1_H$
- 2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$