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, $y \in S$, $y \sim x$.*
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 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* $\cdot$*".*

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* $\cdot$*).*
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* $\cdot$*).*

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

Definition 3.5 (Left and Right Cosets)**.** *Let* G *be a group and* $H \leq G$*. For* $g \in G$*:*

$$\begin{aligned} gH &= \{gh : h \in H\} \quad \textit{(left coset)} \\ Hg &= \{hg : h \in H\} \quad \textit{(right coset).} \end{aligned}$$

Proposition 3.1. *For a subgroup* $H \leq G$*, the collection of left cosets* $\{gH : g \in G\}$ *forms a partition of* G*. Similarly, the collection of right cosets* $\{Hg : g \in G\}$ *also forms a partition of* 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 (Index)**.** *The* index *of a subgroup* H *in* G*, denoted* $[G : H]$*, is the number of distinct left cosets of* H *in* G*.*

Definition 3.7 (Order of an Element). *Let G be a group and $g \in G$. The* order *of g, denoted $|g|$, is the smallest positive integer n such that*

$$g^n = e,$$

where e is the identity element of G.

If no such n exists, then g is said to have infinite order.

Definition 3.8 (Normal Subgroup). *A subgroup $N \leq G$ is called a* normal subgroup*, written $N \trianglelefteq G$, if*

$$gN = Ng \quad \text{for all } g \in G.$$

Equivalently, N is normal if

$$gNg^{-1} = N \quad \text{for all } g \in G.$$

Proposition 3.2. *If $N \trianglelefteq G$, then the set of cosets $G/N = \{gN : g \in G\}$ forms a group under the operation*

$$(gN)(hN) = (gh)N.$$

This group is called the quotient group *of G by N.*

4 Group Homomorphisms

Definition 4.1 (Group Homomorphism). *A function $\varphi : G \to H$ between groups is called a* homomorphism *if*

$$\varphi(ab) = \varphi(a)\varphi(b) \quad \text{for all } a, b \in G.$$