MATH 327: Algebra 1

Lecture 1 — Groups and subgroups

Manish Patnaik

Compiled August 25, 2026

1 Groups

Definition 1.1. A *group* is a set G together with a binary operation $\cdot : G \times G \to G$ satisfying:

1. (Associativity) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$.
2. (Identity) There exists $e \in G$ with $e \cdot a = a \cdot e = a$ for all $a \in G$.
3. (Inverses) For each $a \in G$ there is $a^{-1} \in G$ with $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Proposition 1.2. *The identity element of a group is unique.*

Proof. Suppose e and e' both satisfy the identity axiom. Then $e = e \cdot e' = e'$, where the first equality uses that e' is an identity and the second that e is. □

2 Subgroups

Definition 2.1. A subset $H \subseteq G$ is a *subgroup*, written $H \leq G$, if H is closed under the operation, contains e, and is closed under inverses.