Abstract Algebra: A Dense, Self-contained Lecture

From Groups to Polynomial Rings and Cyclic Codes

Khushraj Madnani (lecture slides)

October 30, 2025

Outline

Introduction & Motivation

What is Abstract Algebra?

Definition
An *algebraic structure* is a set equipped with one or more operations that satisfy a collection of axioms (closure, associativity, etc.).

- Central theme: study *structure preservation* under operations.
- Running examples: $\mathbb{Z}_n$ (modular addition), symmetry groups of polygons, polynomial rings $\mathbb{F}[x]$.

Notation and Conventions

- Group $(G, \cdot)$: we write multiplicatively by default; additively when convenient $(G, +)$.
- For an element $g \in G$, g^n denotes repeated product; $\langle g \rangle$ denotes subgroup generated by g.
- Rings are unital unless otherwise stated; $0, 1$ denote additive and multiplicative identities.

Course Goals

Dense, self-contained coverage such that:

- Definitions, theorems, and full proofs appear in the slides.
- Non-trivial examples included for each major result.
- Minimal external reference required.

Groups

Definition

A *group* $(G, *)$ is a set G with a binary operation $*$ satisfying:

1. (Closure) $\forall a, b \in G,\ a * b \in G$.
2. (Associativity) $\forall a, b, c \in G,\ (a * b) * c = a * (b * c)$.
3. (Identity) $\exists e \in G$ such that $\forall a \in G,\ e * a = a = a * e$.
4. (Inverse) $\forall a \in G, \exists a^{-1} \in G$ with $a * a^{-1} = e = a^{-1} * a$.

Theorem
Identity and inverses in a group are unique.

Proof.
If e, e' are identities then $e = e * e' = e'$. For uniqueness of inverse, if b and c are inverses of a, then $b = b * e = b * (a * c) = (b * a) * c = e * c = c$. $\square$

Examples of Groups

Example
$(\mathbb{Z}, +)$ is a group with identity 0 and inverse $-n$ for $n \in \mathbb{Z}$.

Example
$(\mathbb{Z}_n, +_n)$: integers mod n under addition. Finite group with n elements.

Example
S_n, the symmetric group on n letters (all permutations) with composition.

Order of an Element and Lagrange's Motivation

Definition
The *order* of $g \in G$ is the smallest positive integer m such that $g^m = e$, if it exists; otherwise order is infinite.

Note: orders of elements divide group order in finite groups (Lagrange). We'll prove this later.

Cyclic Groups

Definition
A group G is *cyclic* if $\exists g \in G$ such that $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Example
$\mathbb{Z}_n$ is cyclic generated by 1.

Cayley Tables: Visualizing Group Operations

- The **Cayley table** of a finite group $G = \{g_1, g_2, \ldots, g_n\}$ lists all products $g_i g_j$ in a table form.
- Each row and column correspond to group elements; the entry at row i, column j is $g_i g_j$.

Properties:

- The identity element e appears once in each row and each column.
- Each row and column is a permutation of the group elements (Latin square property).
- Associativity can be verified indirectly by checking consistency of the table.

Example: Cayley Table of $C_3 = \{e, a, a^2\}$ where $a^3 = e$.

Subgroups, Generators and Powers

Subgroup Definition and Tests

Definition
A subset $H \subseteq G$ is a *subgroup* (denoted $H \leq G$) if H itself is a group under the operation of G.

Proposition (One-step subgroup test)
A non-empty subset $H \subseteq G$ is a subgroup iff $\forall a, b \in H,\ ab^{-1} \in H$.

Subgroup Definition and Tests

Definition
A subset $H \subseteq G$ is a *subgroup* (denoted $H \leq G$) if H itself is a group under the operation of G.

Proposition (One-step subgroup test)
A non-empty subset $H \subseteq G$ is a subgroup iff $\forall a, b \in H,\ ab^{-1} \in H$.

Proof.
If H is a subgroup the condition holds. Conversely, taking $b = a$ gives $aa^{-1} = e \in H$, closure follows from $ab^{-1} \in H$, and inverses follow by choosing suitable a, b. $\square$

Generated Subgroups and Intersections

Definition
For $S \subseteq G$, $\langle S \rangle$ is the smallest subgroup containing S, equivalently the intersection of all subgroups of G that contain S.

Proposition
Intersection of any family of subgroups is a subgroup.

Generated Subgroups and Intersections

Definition
For $S \subseteq G$, $\langle S \rangle$ is the smallest subgroup containing S, equivalently the intersection of all subgroups of G that contain S.

Proposition
Intersection of any family of subgroups is a subgroup.

Proof.
Direct verification using the subgroup test; non-emptiness is ensured as all subgroups contain e. $\square$

Orders in Cyclic Groups

Theorem
If $G = \langle g \rangle$ is finite cyclic and $|G| = n$, then $g^k = e \iff n \mid k$. Moreover, the order of g is n and $\langle g^d \rangle$ has order $n/\gcd(n, d)$.

Orders in Cyclic Groups

Theorem

If $G = \langle g \rangle$ is finite cyclic and $|G| = n$, then $g^k = e \iff n \mid k$. Moreover, the order of g is n and $\langle g^d \rangle$ has order $n/\gcd(n, d)$.

Proof.

Basic number theory: $g^k = e$ implies $n \mid k$ by minimality of n. For subgroup generated by g^d, its order is $n/\gcd(n, d)$ by considering multiples. $\square$

Examples: Subgroups of $\mathbb{Z}_n$

Subgroups correspond to divisors: for each $d \mid n$, $\langle n/d \rangle$ is a subgroup of order d. Hence lattice of subgroups is isomorphic to divisibility lattice of n.

Cosets and Lagrange's Theorem

Cosets

Definition
For $H \leq G$ and $g \in G$, the left coset $gH = \{gh : h \in H\}$. Right coset Hg analogously.

Properties: all left cosets have same cardinality as H, they partition G.

Partitioning by Cosets

If $g_1H \cap g_2H \neq \emptyset$ then $g_1H = g_2H$. Hence left cosets partition G into disjoint equal-sized blocks.

Lagrange's Theorem

Theorem
If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$. Precisely, $|G| = |H|\,[G : H]$ where $[G : H]$ is number of left cosets.

Lagrange's Theorem

Theorem
If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$. Precisely, $|G| = |H| \, [G : H]$ where $[G : H]$ is number of left cosets.

Proof.
Partition G into $[G : H]$ cosets each of size $|H|$; count elements. $\square$

Consequences of Lagrange

Corollary
If G is finite and $a \in G$, then $\mathrm{ord}(a) \mid |G|$.

Consequences of Lagrange

Corollary
If G is finite and $a \in G$, then $\mathrm{ord}(a) \mid |G|$.

Proof.
$\langle a \rangle$ is a subgroup whose order equals $\mathrm{ord}(a)$, apply Lagrange. $\square$

Example and Exercise

Example: In $\mathbb{Z}_{12}$, subgroup $\langle 4 \rangle = \{0, 4, 8\}$ has order 3; there are 4 cosets.

Exercise: Prove that any group of prime order p is cyclic.

Example and Exercise

Example: In $\mathbb{Z}_{12}$, subgroup $\langle 4 \rangle = \{0, 4, 8\}$ has order 3; there are 4 cosets.

Exercise: Prove that any group of prime order p is cyclic.

Proof.
Let $|G| = p$. For any $a \neq e$, $\text{ord}(a)$ divides p and is > 1, so equals p, thus $G = \langle a \rangle$. $\square$

Homomorphisms and Normal Subgroups

Group Homomorphisms

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

Kernel $\ker \varphi = \{g \in G : \varphi(g) = e\}$, image $\operatorname{im} \varphi = \varphi(G)$. Intuitive explanation of Kernel to be discussed in class.

Isomorphisms and Automorphisms

Isomorphisms

Definition
An *isomorphism* $\varphi : G \to H$ is a bijective homomorphism: $\varphi(ab) = \varphi(a)\varphi(b)$.

Isomorphic groups are structurally identical; notation $G \cong H$.

Properties Preserved by Isomorphism

If $\varphi : G \to H$ is isomorphism then:

- $|G| = |H|$ (finite case)
- $\text{ord}(a) = \text{ord}(\varphi(a))$
- Subgroup lattice structure preserved

Automorphism Group

Definition
$\mathrm{Aut}(G) = \{\varphi : G \to G \mid \varphi \text{ is an isomorphism}\}$, a group under composition.

Example: $\mathrm{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}_n)^\times$.