Abstract Algebra

December 19, 2025

Notes here are based on Pinter - A Book of Abstract Algebra, 2nd Edition. I focused on just definitions and key theorems, unlike my Linear Algebra notes where I feel like I way overdid it.

1 Algebras

Every **algebra** consists of a set and certain operations on that set.

An **algebraic structure** is a set with one or more operations defined on it.

2 Operations

An **operation** $\circ$ on A is a rule which assigns to each ordered pair (a, b) of elements of A exactly one element $a \circ b$ in A.

2.1 Algebraic Properties

Properties of operations on a set A:

- **Closure**: The operation on elements in A always produces another element of A.
- **Commutativity**: $a \circ b = b \circ a$ for any two elements a and b in A.
- **Associativity**: $(a \circ b) \circ c = a \circ (b \circ c)$ for any three elements a, b, c in A.

Other algebraic properties include existence of an identity/neutral element, existence of an inverses of all elements, and distributivity (which applies to structures with multiple operations). More on all these to follow.

2.2 Neutral Element

If there exists an element e in A such that

$e \circ a = a$ and $a \circ e = a$ for every a in A

we call e an **identity element** aka **neutral element** for the operation $\circ$.

0 is identity element for addition, 1 for multiplication.

2.3 Inverses

An **inverse** a^{-1} is defined by causing a to reach the neutral element e:

$a \circ a^{-1} = e$ and $a^{-1} \circ a = e$

3 Groups

A **group** is a set G with an operation $\circ$ which satisfies the axioms: 1. $\circ$ is associative. 2. There is an element e in G such that $a \circ e = a$ and $e \circ a = a$ for every element a in G. 3. For every element a in G, there is an element a^1 in G such that $a \circ a^{-1} = e$ and $a^{-1} \circ a = e$.

The notation for the above group would be $\langle G, \circ \rangle$.

Note that the definition of an operation ensures that we always stay within G when performing the operation.

If the commutative law holds in a group G, such a group is called an **abelian group** or a **commutative group**.

The number of elements in a finite group G is called its **order**. It's denoted by $|G|$.

We say that two elements in a group **commute** if $ab = ba$.

The **direct product** of a group $G \times H = \{(x, y) : x \in G \wedge y \in H\}$

Every finite group can be represented by a **Cayley Diagram**. Each point is an element of the group, and the directional arrows indicate the result of multiplying by their generators. Different line colors or dottings can be used to indicate which generator an arrow refers to. There are no arrows when there's bidirectionality because a given generator is its own inverse.

4 Subgroups

Let G be a group, and S a nonempty subset of G. If the product of every pair of elements of S is in S, we say that S is **closed with respect to multiplication**. If the inverse of every element of S is in S, we say that S is **closed with respect to inverses**. If both of these are true, we call S a **subgroup** of G (and itself a group).

In any group G the one-element subset $\{e\}$, containing only the neutral element, is a subgroup. At the other extreme, the whole group G is obviously a subgroup of itself. These two examples are, respectively, the smallest and largest possible subgroups of G. They are called the **trivial subgroups** of G. All the other subgroups of G are called **proper subgroups**.

A **generator** of a group G is a subset $S \subseteq G$ such that every element of G can be expressed as a finite product of elements from S and their inverses.

The **subgroup generated by** a subset S, denoted $\langle S \rangle$, of a group G is the smallest subgroup of G containing S, equivalently the set of all finite products of elements of S and their inverses.

A concise definition of the subgroup generated by a could be given by:

$$\langle a \rangle := \left\{ a^k \mid k \in \mathbb{Z} \right\}$$

A set of equations, involving only the generators (which includes their inverses), is called a set of **defining equations** for G if these equations completely determine the table of G.

By the **center** of a group G we mean the set of all the elements of G which commute with every element of G, that is,

$$C = \{a \in G : ax = xa \text{ for every } x \in G\}$$

5 Groups of Permutations

A **permutation** of a set A is a bijection $A \to A$.

Because composite bijections are themselves a bijection, the composite of any two permutations is a permutation.

The set of all permutations of A with the operation $\circ$ of composition, is a group. The group of all permutations for a given set A is called the **symmetric group** on A. The symmetric group on n elements is denoted by S_n.

The **dihedral group**, denoted D_n corresponds to the group of symmetries of an n-gon. These symmetries consist of rotation and reflection subgroups.

See the symmetries of a square. Rotations are like if you stuck a pole through it like a pig on a spit.

6 Permutations of a Finite Set

Let $a_1, a_2, \ldots, a_s$ be distinct elements of the set $\{1, 2, \ldots, n\}$. By the **cycle** $(a_1 a_2 \ldots a_s)$ we mean the permutation of $\{1, 2, \ldots, n\}$ which carries a_1 to a_2, a_2 to a_3,…, a_{s-1} to a_s, and a_s to a_1, while leaving all the remaining elements of $\{1, 2, \ldots, n\}$ fixed. (Note the conection with modular addition: a cycle maps a_i $a_{i+1 \mod s}$

Because cycles are permutations, we may form the **composite** of two cycles in the usual manner. The composite of cycles is generally called their **product** and it is customary to omit the symbol $\circ$.

If $(a_1 a_2 \ldots a_s)$ is a cycle, the integer s is called its **length**; thus, $(a_1 a_2 \ldots a_s)$ is a cycle of length s.

If two cycles have no elements in common they are said to be **disjoint**. Disjoint cycles commute.

Theorem: Every permutation is either the identity, a single cycle, or a product of disjoint cycles (unique up to reordering the cycles and cyclic shifts within cycles).

A cycle of length 2 is called a **transposition**. Every cycle can be expressed as a product of one or more transpositions. In fact,

$$(a_1 a_2 \ldots a_r) = (a_r a_{r-1})\,(a_r a_{r-2}) \ldots (a_r a_3)\,(a_r a_2)\,(a_r a_1)$$

However, the expression of a permutation as a product of transpositions is not unique, and even the number of transpositions involved is not unique. Nevertheless, when a permutation is written as a product of transpositions, one property of this expression is unique: the number of transpositions involved is either always even or always odd. A permutation is called **even** if it is a product of an even number of transpositions, and **odd** if it is a product of an odd number of transpositions.

Theorem: The identity permutation is even.

When you take the product of two permutations, the oddness or evennness of the composite permutation follows the same rule as odd/even for addition. Two odds or evens compose to an even, and one odd and one even compose to an odd.

The set of all the even permutations in S_n is a subgroup of S_n. It is called the **alternating group**, and is denoted by A_n.

If α is any permutation, the least positive integer n such that $\alpha^n = \epsilon$ is called the **order** of α.

6.1 Powers of Permutations

Let α be a cycle of length s.

There will be s distinct powers of α. α^s will be the identity permutation. α^{s-1} will be α^{-1}.

α^2 is a cycle iff s is odd. If s is odd, the square root of α will be $\alpha^{\frac{s+1}{2}}$ (this follows from the fact that $\alpha = \alpha^{s+1}$).

Cycle Decomposition Theorem: α^k is the product of $d = \gcd(s, k)$ disjoint cycles of length $t = \frac{s}{d}$. Specifically:

$$\alpha^k = \prod_{m=1}^{d} (m, m+k, m+2k, \ldots, m+(t-1)k)$$

From this we can see that when s and k are coprime ($\gcd(s, k) = 1$), α^k will be a single cycle. Furthmore, when s is prime, the only possible $\gcd(s, k)$ is either 1 (another single cycle) or s, in which case we have cycles of length 1 – resulting in the identity permutation.

6.2 Conjugate Cycles

If α is any cycle, and π any permutation, $\pi\alpha\pi^{-1}$ is called the **conjugate**.

The conjugate of α is the cycle which "labels" the cycle, $(\pi(\alpha_1), \ldots, \pi(\alpha_s))$

When we say two cycles are conjugates of each other, we mean that there exists a permutation such that one cycle can be transformed into the other by relabeling its elements. Note that the inverse of that permutation gets things to work in the opposite direction.

Any two cycles of equal length are conjugates of each other.

Let σ be a product $\alpha_1 \ldots \alpha_t$ of t disjoint cycles of lengths $l_1 \ldots, l_t$, respectively. Then $\pi\sigma\pi^{-1}$ is also a product of t disjoint cycles of lengths $l_1, \ldots, l_t$. The proof for this involves the observation that

$$\pi\sigma\pi^{-1} = \pi a_1 a_2 \cdots a_t \pi^{-1} = \left(\pi a_1 \pi^{-1}\right)\left(\pi a_2 \pi^{-1}\right) \cdots \left(\pi a_t \pi^{-1}\right).$$

6.3 Order of Cycles

If α is any permutation, the least positive integer n such that $\alpha^n = \epsilon$ is called the order of α.

If α is any cycle of length s, the order of α is s.

If α and β are disjoint cycles of lengths r and s, respectively, the order of $\alpha\beta$ is $\operatorname{lcm}(\alpha\beta)$.

7 Isomorphism

Isomorphic things have the same structure.

Let G_1 and G_2 be groups. A bijective function $f : G_1 \to G_2$ with the property that for any two elements a and b in G_1,

$$f(ab) = f(a)f(b)$$

is called an **isormophism** from G_1 to G_2. If there exists an isomorphism from G_1 to G_2, we say that G_1 is **isormophic** to G_2.

Notation for congruence is $G_1 \cong G_2$.

Cayley's Theorem: Every group is isomorphic to a group of permutations. (Recall that a group of permutations is a subgroup of S_n.)

7.1 Isomorphism Is an Equivalence Relation Among Groups

Every group is isomorphic to itself. If $G_1 \cong G_2$, then $G_2 \cong G_1$. If $G_1 \cong G_2$ and $G_2 \cong G_3$, then $G_1 \cong G_3$.

The identity function is always an isomorphism from a group to itself.

7.2 Elements Which Correspond under an Isomorphism

If we have an isomorphism $f : G_1 \to G_2$:

- f matches the neutral element of G_1 with the neutral element of G_2.
- If f matches an element x in G_1 with y in G_2, then f matches x^{-1} with y^{-1}.
- f matches a generator of G_1 with a generator of G_2.

7.3 Some General Properties of Isomorphism

- $G \times H \cong H \times G$
- If $G_1 \cong G_2$ and $H_1 \cong H_2$, then $G_1 \times H_1 \cong G_2 \times H_2$
- G is abelian iff $f(x) = x^{-1}$ is an isomorphism from G to G.

7.4 Group Automorphisms

If G is a group, an **automorphism** of G is an isomorphism from G to G. The identity function is always an automorphism of a group, but there can be others beside this obvious one.

Since each automorphism of G is a bijective function from G to G, it is a permutation of G.

7.5 Regular Representation of Groups

By Cayley's theorem, every group G is isomorphic to a group G^* of permutations of G. Recall that we match each element a in G with the permutation $\pi_a = ax$, that is, "multiply on the left by a." We let $G^* = \{\pi_a : a \in G\}$; with the operation $\circ$ of composition it is a group of permutatiojns, called the **left regular representation** of G. It is called a "representation" of G because it is isomorphic to G.

Instead of using the permutations π_a, we could just as well have used the permutations ρ_a, defined by $\rho_a(x) = xa$, that is, "multiply on the right by a. The group $G^\rho = \{\rho_a : a \in G\}$ is called the **right regular representation** of G.

If G is commutative, there is no difference between the right and left multiplication, so G^* and G^ρ are the same, and are simply called the **regular representation** of G.

8 Order of Group Elements

Let G be a group, and a and element of G. If there exists a nonzero integer m such that $a^m = e$, then there exists a positive integer n such that $a^n = e$. Specifically, if $m < 0$, then $m = -n$ works because $e^{-1} = e$.

If there exists a nonzero integer m such that $a^m = e$, then the **order** of the element a is defined to be the least positive integer n such that $a^n = e$. If there does not exist any nonzero integer m such that $a^m = e$, we say that a has order infinity.

The finite order of an element g of a group can be defined as:

$$\operatorname{ord}(g) = \min \left\{ k \in \mathbb{N} \mid g^k = e \right\}$$

Thus, in any group G, every element has an order which is either a positive integer or infinity. If the order of a is a positive integer, we say that a has **finite order**, otherwise a has **infinite order**.

In the following theorems, G is an arbitrary group, and a is any element of G.

Theorem: if a has finite order n, there are exactly n different powers of a, namely:

$$a^0, a, a^2, a^3, \ldots, a^{n-1}$$

What this theorem asserts is that every positive or negative power of a is equal to one of the above, and the above are all different from one another.

Theorem: If a has infinite order, then all the powers of a are different. That is, if r and s are distinct integers, then $a^r \neq a^s$.

Theorem: Suppose an element a in a group has order n. Then $a^t = e$ iff t is a multiple of n.

8.1 Elementary Properties of Order

Let a, b, and c be elements of a group G. Then:

$\operatorname{ord}(a) = \operatorname{ord}(bab^1)$

The order of a^1 is the same as the order of a.

The order of ab is the same as the order of ba.

$\operatorname{ord}(abc) = \operatorname{ord}(cab) = \operatorname{ord}(bca)$.

Let $x = a^1 a^2 \cdots a^n$, and let y be a product of the same factors, permuted cyclically. (That is, $y = a_k a_{k+1} \cdots a_n a_1 \cdots a_{k-1}$.) Then $\operatorname{ord}(x) = \operatorname{ord}(y)$.

8.2 Further Properties of Order

If $a^p = e$ where p is a prime number, then a has order p. $(a \neq e)$.

The order of a^k is a divisor (factor) of the order of a.

If $\operatorname{ord}(a) = km$, then $\operatorname{ord}\left(a^k\right) = m$.

If $\operatorname{ord}(a) = n$ where n is odd, then $\operatorname{ord}\left(a^2\right) = n$.

8.3 Relationship between ord(ab), ord(a), and ord(b)

Let a and b be elements of a group G. Let $\text{ord}(a) = m$ and $\text{ord}(b) = n$; let $\text{lcm}(m,\ n\ )$ denote the least common multiple of m and n.

If a and b commute, then $\text{ord}(ab)$ is a divisor of $\text{lcm}(m, n)$.

If m and n are relatively prime, then no power of a can be equal to any power of b (except for e). (REMARK: Two integers are said to be relatively prime if they have no common factors except ± 1.)

If m and n are relatively prime, then the products $a^i b^j (0 \leq i < m, 0 \leq j < n)$ are all distinct.

Let a and b commute. If m and n are relatively prime, then $\text{ord}(ab) = mn$.

Let a and b commute. There is an element c in G whose order is $\text{lcm}(m, n)$.

Thus, there is no simple relationship between $\text{ord}(ab)$, $\text{ord}(a)$, and $\text{ord}(b)$ if a and b fail to commute.

8.4 Relationship between ord(a) and ord(aˆk)