

# Part I

## Abstract Algebra

## Definition

Given a set  $G$  and a binary operation  $*$  on  $G$ . For any elements  $a, b$ , and  $c$  in  $G$

- 1 Closure:  $a * b \in G$
- 2 Associative:  $(a * b) * c = a * (b * c)$
- 3 Identity: a unique element  $e \in G$  such that
$$\Rightarrow a * e = e * a = a$$
- 4 Inverse: an element  $a' \in G$  of  $a$ , written as  $a^{-1}$ , such that
$$\Rightarrow a * a' = a' * a = e, \text{ or}$$
$$\Rightarrow a * a^{-1} = a^{-1} * a = e$$
- 5 Commutative:  $a * b = b * a$

## Definition

Given a set  $G$  and a binary operation  $*$  on  $G$ . For any elements  $a, b$ , and  $c$  in  $G$

- ① Closure:  $a * b \in G$
- ② Associative:  $(a * b) * c = a * (b * c)$
- ③ Identity: a unique element  $e \in G$  such that
$$\Rightarrow a * e = e * a = a$$
- ④ Inverse: an element  $a' \in G$  of  $a$ , written as  $a^{-1}$ , such that
$$\Rightarrow a * a' = a' * a = e, \text{ or}$$
$$\Rightarrow a * a^{-1} = a^{-1} * a = e$$
- ⑤ Commutative:  $a * b = b * a$

## Definition

Given a set  $G$  and a binary operation  $*$  on  $G$ . For any elements  $a, b$ , and  $c$  in  $G$

- 1 Closure:  $a * b \in G$
- 2 Associative:  $(a * b) * c = a * (b * c)$
- 3 Identity: a unique element  $e \in G$  such that

$$\text{👉 } a * e = e * a = a$$

- 4 Inverse: an element  $a' \in G$  of  $a$ , written as  $a^{-1}$ , such that


$$\Rightarrow a * a' = a' * a = e, \text{ or}$$

$$\Rightarrow a * a^{-1} = a^{-1} * a = e$$

- 5 Commutative:  $a * b = b * a$

## Definition

Given a set  $G$  and a binary operation  $*$  on  $G$ . For any elements  $a, b$ , and  $c$  in  $G$

- ① Closure:  $a * b \in G$
- ② Associative:  $(a * b) * c = a * (b * c)$
- ③ Identity: a unique element  $e \in G$  such that  
  $a * e = e * a = a$
- ④ Inverse: an element  $a' \in G$  of  $a$ , written as  $a^{-1}$ , such that  
 $\Rightarrow a * a' = a' * a = e$ , or  
 $\Rightarrow a * a^{-1} = a^{-1} * a = e$
- ⑤ Commutative:  $a * b = b * a$

## Definition

Given a set  $G$  and a binary operation  $*$  on  $G$ . For any elements  $a, b$ , and  $c$  in  $G$

- ① Closure:  $a * b \in G$
- ② Associative:  $(a * b) * c = a * (b * c)$
- ③ Identity: a unique element  $e \in G$  such that
  - ♪  $a * e = e * a = a$
- ④ Inverse: an element  $a' \in G$  of  $a$ , written as  $a^{-1}$ , such that
  - 👉  $a * a' = a' * a = e$ , or
  - 👉  $a * a^{-1} = a^{-1} * a = e$
- ⑤ Commutative:  $a * b = b * a$

## Definition

Given a set  $G$  and a binary operation  $*$  on  $G$ . For any elements  $a, b$ , and  $c$  in  $G$

- ① Closure:  $a * b \in G$
- ② Associative:  $(a * b) * c = a * (b * c)$
- ③ Identity: a unique element  $e \in G$  such that
  - ♪  $a * e = e * a = a$
- ④ Inverse: an element  $a' \in G$  of  $a$ , written as  $a^{-1}$ , such that
  - 🔴  $a * a' = a' * a = e$ , or
  - ♪  $a * a^{-1} = a^{-1} * a = e$
- ⑤ Commutative:  $a * b = b * a$

## Definition

Given a set  $G$  and a binary operation  $*$  on  $G$ . For any elements  $a, b$ , and  $c$  in  $G$

- 1 Closure:  $a * b \in G$
- 2 Associative:  $(a * b) * c = a * (b * c)$
- 3 Identity: a unique element  $e \in G$  such that
  - 🎵  $a * e = e * a = a$
- 4 Inverse: an element  $a' \in G$  of  $a$ , written as  $a^{-1}$ , such that
  - 🎵  $a * a' = a' * a = e$ , or
  - 👉  $a * a^{-1} = a^{-1} * a = e$
- 5 Commutative:  $a * b = b * a$



## Definition

Given a set  $G$  and a binary operation  $*$  on  $G$ . For any elements  $a, b$ , and  $c$  in  $G$

- ① Closure:  $a * b \in G$
- ② Associative:  $(a * b) * c = a * (b * c)$
- ③ Identity: a unique element  $e \in G$  such that
  - ♪  $a * e = e * a = a$
- ④ Inverse: an element  $a' \in G$  of  $a$ , written as  $a^{-1}$ , such that
  - ♪  $a * a' = a' * a = e$ , or
  - ♪  $a * a^{-1} = a^{-1} * a = e$
- ⑤ Commutative:  $a * b = b * a$

\_\_\_\_\_

---

## Definition $(G, *)$

A nonempty set  $G$  with a binary operation  $*$  is called

🎵 Groupoid,

👉 if (1) is true

♪ Semigroup,

♪ Monoid,

Group,

\_\_\_\_\_

...and the  $\beta$  parameter is estimated by the following equation:

1000

1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 2680, 26

---

## Definition $(G, *)$

A nonempty set  $G$  with a binary operation  $*$  is called

- Groupoid,
  - if (1) is true
- Semigroup,
  - if (1)-(2) are true
- Monoid,
  - if (1)-(3) are true
- Group,
  - if (1)-(4) are true
- Abelian groupoid (semigroup, monoid, group),
  - if (5) is true

## Definition $(G, *)$

A nonempty set  $G$  with a binary operation  $*$  is called

♪ Groupoid,

🎵 if (1) is true

🎵 Semigroup,

- if (1)-(2) are true

➡ Monoid,

👉 if (1)-(3) are true

Group,

## Definition $(G, *)$

A nonempty set  $G$  with a binary operation  $*$  is called

- Groupoid,
  - if (1) is true
- Semigroup,
  - if (1)-(2) are true
- Monoid,
  - if (1)-(3) are true
- Group,
  - if (1)-(4) are true
- Abelian groupoid (semigroup, monoid, group),
  - if (5) is true

\_\_\_\_\_

...and the  $\beta$  parameter is estimated by the following equation:



100

1. *Journal of the American Medical Association*, 1997; 277: 1039-1043.

- ♪ Groupoid,
  - ♪ if (1) is true
- ♪ Semigroup,
  - ♪ if (1)-(2) are true
- ♪ Monoid,
  - ♪ if (1)-(3) are true
- ♪ Group,
  - 👉 if (1)-(4) are true
- ♪ Abelian groupoid (semigroup, monoid, group),
  - 👉 if (5) is true

## Definition $(G, *)$

A nonempty set  $G$  with a binary operation  $*$  is called

- ♪ Groupoid,

- 🎵 if (1) is true

- ♪ Semigroup,

- if (1)-(2) are true

- ♪ Monoid,

- if (1)-(3) are true

- Group,

- if (1)-(4) are true

- 👉 Abelian groupoid (semigroup, monoid, group),

## Definition $(G, *)$

A nonempty set  $G$  with a binary operation  $*$  is called

- ♪ Groupoid,
  - ♪ if (1) is true
- ♪ Semigroup,
  - ♪ if (1)-(2) are true
- ♪ Monoid,
  - ♪ if (1)-(3) are true
- ♪ Group,
  - ♪ if (1)-(4) are true
- ♪ Abelian groupoid (semigroup, monoid, group),
  - 👉 if (5) is true

## Theorem (Associativity)

♪ If  $a_1, a_2, \dots, a_n, n \geq 3$ , are arbitrary elements of a semigroup, then all products of the elements  $a_1, a_2, \dots, a_n$  that can be formed by inserting meaningful parentheses arbitrarily are equal.

## Notice

♪ The Theorem shows that the products are all equal.

$$♪ ((a_1 * a_2) * a_3) * a_4$$

$$♪ a_1 * (a_2 * (a_3 * a_4))$$

$$♪ (a_1 * (a_2 * a_3)) * a_4$$

♪ If  $a_1, a_2, \dots, a_n$  are elements in a semigroup  $(S, *)$ , then the product can be written as

$$♪ a_1 * a_2 * \dots * a_n$$

## Theorem (Associativity)

♪ If  $a_1, a_2, \dots, a_n, n \geq 3$ , are arbitrary elements of a semigroup, then all products of the elements  $a_1, a_2, \dots, a_n$  that can be formed by inserting meaningful parentheses arbitrarily are equal.

## Notice

♪ The Theorem shows that the products are all equal.

$$♪ ((a_1 * a_2) * a_3) * a_4$$

$$♪ a_1 * (a_2 * (a_3 * a_4))$$

$$♪ (a_1 * (a_2 * a_3)) * a_4$$

♪ If  $a_1, a_2, \dots, a_n$  are elements in a semigroup  $(S, *)$ , then the product can be written as

$$♪ a_1 * a_2 * \dots * a_n$$

$(\mathbb{Z}, +)$ ♪  $\mathbb{Z}$ : the set of all integers♪  $+$ : ordinary addition $(\mathbb{Z}, -)$ ♪  $\mathbb{Z}$ : the set of all integers♪  $-$ : ordinary subtraction $(\mathcal{P}(S), \cup)$ ♪  $(\mathcal{P}(S))$ : the powerset of  $S$ ♪  $\cup$ : union operation on sets

$(\mathbb{Z}, +)$ ♪  $\mathbb{Z}$ : the set of all integers♪  $+$ : ordinary addition $(\mathbb{Z}, -)$ ♪  $\mathbb{Z}$ : the set of all integers♪  $-$ : ordinary subtraction $(\mathcal{P}(S), \cup)$ ♪  $(\mathcal{P}(S))$ : the powerset of  $S$ ♪  $\cup$ : union operation on sets

$(\mathbb{Z}, +)$ 

- ♪  $\mathbb{Z}$ : the set of all integers
- ♪  $+$ : ordinary addition

 $(\mathbb{Z}, -)$ 

- ♪  $\mathbb{Z}$ : the set of all integers
- ♪  $-$ : ordinary subtraction

 $(\mathcal{P}(S), \cup)$ 

- ♪  $(\mathcal{P}(S))$ : the powerset of  $S$
- ♪  $\cup$ : union operation on sets



## Definition (Let $A = \{a_1, a_2, \dots, a_n\}$ be an alphabet)

♪ Let

♪  $A^*$  is the set of all finite sequences of elements of  $A$ .

♪  $\alpha, \beta$ , and  $\gamma$  be elements of  $A^*$ .

♪ The catenation is a binary operation  $\cdot$  on  $A^*$ .

👉 if  $\alpha = a_{i_1} a_{i_2} \dots a_{i_s}$  and  $\beta = a_{j_1} a_{j_2} \dots a_{j_t}$ , then

$$\blacklozenge \alpha \cdot \beta = a_{i_1} a_{i_2} \dots a_{i_s} a_{j_1} a_{j_2} \dots a_{j_t}$$

$$\text{♪ } \alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$$

## Definition (Let $A = \{a_1, a_2, \dots, a_n\}$ be an alphabet)

♪ Let

♪  $A^*$  is the set of all finite sequences of elements of  $A$ .

♪  $\alpha, \beta$ , and  $\gamma$  be elements of  $A^*$ .

♪ The catenation is a binary operation  $\cdot$  on  $A^*$ .

♪ if  $\alpha = a_{i_1} a_{i_2} \dots a_{i_s}$  and  $\beta = a_{j_1} a_{j_2} \dots a_{j_t}$ , then

$$\blacklozenge \alpha \cdot \beta = a_{i_1} a_{i_2} \dots a_{i_s} a_{j_1} a_{j_2} \dots a_{j_t}$$

$$\text{♪ } \alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$$

## Definition (Let $A = \{a_1, a_2, \dots, a_n\}$ be an alphabet)

♪ Let

♪  $A^*$  is the set of all finite sequences of elements of  $A$ .

♪  $\alpha, \beta$ , and  $\gamma$  be elements of  $A^*$ .

♪ The catenation is a binary operation  $\cdot$  on  $A^*$ .

♪ if  $\alpha = a_{i_1} a_{i_2} \dots a_{i_s}$  and  $\beta = a_{j_1} a_{j_2} \dots a_{j_t}$ , then

$$\blacklozenge \alpha \cdot \beta = a_{i_1} a_{i_2} \dots a_{i_s} a_{j_1} a_{j_2} \dots a_{j_t}$$

$$\text{👉 } \alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$$

## Theorem (Free Semigroup)

♪  $(A^*, \cdot)$  is a semigroup

♪ called the free semigroup generated by  $A$

## Example

♪ Let

♪  $G$  be the set of all nonzero real numbers, and

♪  $a * b = ab/2$

♪ Show

♪  $(G, *)$  is an Abelian group

Proof.  $*$  is a binary operation.

♪ If  $a$  and  $b$  are elements of  $G$ , then  $ab/2$  is a nonzero real number and hence is in  $G$ .



## Example

♪ Let

♪  $G$  be the set of all nonzero real numbers, and

♪  $a * b = ab/2$

♪ Show

♪  $(G, *)$  is an Abelian group

## Proof. Associativity.

♪  $(a * b) * c = (ab/2) * c = (ab)c/4$

♪  $a * (b * c) = a * (bc/2) = a(bc)/4 = (ab)c/4$

♪  $*$  is associative



## Example

♪ Let

♪  $G$  be the set of all nonzero real numbers, and

♪  $a * b = ab/2$

♪ Show

♪  $(G, *)$  is an Abelian group

Proof. 2 is the identity.

$$♪ a * 2 = (a)(2)/2 = a = (2)(a)/2 = 2 * a$$



## Example

♪ Let

♪  $G$  be the set of all nonzero real numbers, and

♪  $a * b = ab/2$

♪ Show

♪  $(G, *)$  is an Abelian group

Proof.  $a' = 4/a$  is an inverse of  $a$ .

♪ 
$$a * a' = a * 4/a = a(4/a)/2 = 2 = (4/a)(a)/2 = (4/a) * a = a' * a$$





## Example

♪ Let

♪  $G$  be the set of all nonzero real numbers, and

♪  $a * b = ab/2$

♪ Show

♪  $(G, *)$  is an Abelian group

## Proof. Abelian.

♪  $a * b = ab/2 = ba/2 = b * a$



## Example

♪ Let

♪  $G$  be the set of all nonzero real numbers, and

♪  $a * b = ab/2$

♪ Show

♪  $(G, *)$  is an Abelian group

## Proof.

♪ So,  $G$  is an Abelian group.



## Theorem (Uniqueness of Inverse)

♪ *Let  $G$  be a group. Each element  $a \in G$  has only one inverse in  $G$ .*

### Proof.

♪ Let

♪  $a'$  and  $a''$  be inverses of  $a$

♪ Then

$$a' = a'e = a'(aa'') = a'aa'' = (a'a)a'' = ea'' = a''$$



## Theorem (Uniqueness of Inverse)

♪ *Let  $G$  be a group. Each element  $a \in G$  has only one inverse in  $G$ .*

### Proof.

♪ Let

♪  $a'$  and  $a''$  be inverses of  $a$

♪ Then

$$a' = a'e = a'(aa'') = \textcolor{red}{a'aa''} = (a'a)a'' = ea'' = a''$$



## Theorem (Uniqueness of Inverse)

♪ *Let  $G$  be a group. Each element  $a \in G$  has only one inverse in  $G$ .*

### Proof.

♪ Let

♪  $a'$  and  $a''$  be inverses of  $a$

♪ Then

$$a' = a'e = a'(aa'') = a'aa'' = (a'a)a'' = ea'' = a''$$



## Theorem (Uniqueness of Inverse)

♪ *Let  $G$  be a group. Each element  $a \in G$  has only one inverse in  $G$ .*

### Proof.

♪ Let

♪  $a'$  and  $a''$  be inverses of  $a$

♪ Then

$$a' = a'e = a'(aa'') = a'aa'' = (a'a)a'' = ea'' = a''$$



## Theorem (Left/Right Cancellation)

♪ *Let*

♪  *$G$  be a group, and  $a, b$ , and  $c$  be elements of  $G$*

♪ *Then*

♪  *$ab = ac$  implies  $b = c$*

♪  *$ba = ca$  implies  $b = c$*

Proof: Left Cancellation. Suppose that  $ab = ac$ .

♪  $a^{-1}(ab) = a^{-1}(ac)$

♪  $(a^{-1}a)b = (a^{-1}a)c$ , by associativity

♪  $eb = ec$ , by the def. of an inverse

♪  $b = c$  by definition of an identity



## Theorem (Left/Right Cancellation)

♪ Let

♪  $G$  be a group, and  $a, b$ , and  $c$  be elements of  $G$

♪ Then

♪  $ab = ac$  implies  $b = c$

♪  $ba = ca$  implies  $b = c$

Proof: Left Cancellation. Suppose that  $ab = ac$ .

👉  $a^{-1}(ab) = a^{-1}(ac)$

♪  $(a^{-1}a)b = (a^{-1}a)c$ , by associativity

♪  $eb = ec$ , by the def. of an inverse

♪  $b = c$  by definition of an identity





## Theorem (Left/Right Cancellation)

♪ Let

♪  $G$  be a group, and  $a, b$ , and  $c$  be elements of  $G$

♪ Then

♪  $ab = ac$  implies  $b = c$

♪  $ba = ca$  implies  $b = c$

Proof: Left Cancellation. Suppose that  $ab = ac$ .

♪  $a^{-1}(ab) = a^{-1}(ac)$

👉  $(a^{-1}a)b = (a^{-1}a)c$ , by associativity

♪  $eb = ec$ , by the def. of an inverse

♪  $b = c$  by definition of an identity



## Theorem (Left/Right Cancellation)

♪ Let

♪  $G$  be a group, and  $a, b$ , and  $c$  be elements of  $G$

♪ Then

♪  $ab = ac$  implies  $b = c$

♪  $ba = ca$  implies  $b = c$

Proof: Left Cancellation. Suppose that  $ab = ac$ .

♪  $a^{-1}(ab) = a^{-1}(ac)$

♪  $(a^{-1}a)b = (a^{-1}a)c$ , by associativity

🔴  $eb = ec$ , by the def. of an inverse

♪  $b = c$  by definition of an identity



## Theorem (Left/Right Cancellation)

♪ Let

♪  $G$  be a group, and  $a, b$ , and  $c$  be elements of  $G$

♪ Then

♪  $ab = ac$  implies  $b = c$

♪  $ba = ca$  implies  $b = c$

Proof: Left Cancellation. Suppose that  $ab = ac$ .

♪  $a^{-1}(ab) = a^{-1}(ac)$

♪  $(a^{-1}a)b = (a^{-1}a)c$ , by associativity

♪  $eb = ec$ , by the def. of an inverse

👉  $b = c$  by definition of an identity



## Theorem (Inverse of Inverse)

♪ *Let*

♪  *$G$  be a group, and  $a$  and  $b$  be elements of  $G$*

♪ *Then*

$$♪ (a^{-1})^{-1} = a \text{ and } (ab)^{-1} = b^{-1}a^{-1}$$

Proof.



## Theorem (Inverse of Inverse)

♪ *Let*

♪  *$G$  be a group, and  $a$  and  $b$  be elements of  $G$*

♪ *Then*

♪  $(a^{-1})^{-1} = a$  and  $(ab)^{-1} = b^{-1}a^{-1}$

**Proof.**  $(a^{-1})^{-1} = a$ .

♪  $a^{-1}a = aa^{-1} = e$

♪ the inverse of an element is unique,

♪ So,  $(a^{-1})^{-1} = a$



## Theorem (Inverse of Inverse)

♪ Let

♪  $G$  be a group, and  $a$  and  $b$  be elements of  $G$

♪ Then

$$(a^{-1})^{-1} = a \text{ and } (ab)^{-1} = b^{-1}a^{-1}$$

Proof.  $(ab)^{-1} = b^{-1}a^{-1}$ .

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e$$

$$\text{Similarly, } (b^{-1}a^{-1})(ab) = e$$

$$\text{So } (ab)^{-1} = b^{-1}a^{-1}$$



## Theorem (Solution to Equation)

♪ *Let*

♪  *$G$  be a group, and  $a$  and  $b$  be elements of  $G$*

♪ *Then*

♪ *The equation  $ax = b$  has a unique solution in  $G$*

♪ *The equation  $ya = b$  has a unique solution in  $G$*

## Proof.

♪ Omitted



## Definition

- ♪ If  $G$  is a group that has a finite number of elements,  $G$  is said to be a finite group, and the order of  $G$  is the number of elements  $|G|$  in  $G$ .

## Notice

- ♪ A finite group can be represented in the form of the multiplication table.



## Definition

- ♪ If  $G$  is a group that has a finite number of elements,  $G$  is said to be a finite group, and the order of  $G$  is the number of elements  $|G|$  in  $G$ .

## Notice

- ♪ A finite group can be represented in the form of the multiplication table.

## Group of Order 1

 $(\{e\}, *)$ 

$*$	$e$
$e$	$e$

## Group of Order 2

 $(\{e, a\}, *)$ 

$*$	$e$	$a$
$e$	$e$	$a$
$a$	$a$	$e$

## Group of Order 3

 $(\{e, a, b\}, *)$ 

$*$	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$b$	$e$
$b$	$b$	$e$	$a$

## Group of Order 1

 $(\{e\}, *)$ 

$*$	$e$
$e$	$e$

## Group of Order 2

 $(\{e, a\}, *)$ 

$*$	$e$	$a$
$e$	$e$	$a$
$a$	$a$	$e$

## Group of Order 3

 $(\{e, a, b\}, *)$ 

$*$	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$b$	$e$
$b$	$b$	$e$	$a$

## Group of Order 1

 $(\{e\}, *)$ 

$*$	$e$
$e$	$e$

## Group of Order 2

 $(\{e, a\}, *)$ 

$*$	$e$	$a$
$e$	$e$	$a$
$a$	$a$	$e$

## Group of Order 3

 $(\{e, a, b\}, *)$ 

$*$	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$b$	$e$
$b$	$b$	$e$	$a$

## Group of Order 1

 $(\{e\}, *)$ 

$*$	$e$
$e$	$e$

## Group of Order 2

 $(\{e, a\}, *)$ 

$*$	$e$	$a$
$e$	$e$	$a$
$a$	$a$	$e$

## Group of Order 3

 $(\{e, a, b\}, *)$ 

$*$	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$b$	$e$
$b$	$b$	$e$	$a$

## Group of Order 1

 $(\{e\}, *)$ 

$*$	$e$
$e$	$e$

## Group of Order 2

 $(\{e, a\}, *)$ 

$*$	$e$	$a$
$e$	$e$	$a$
$a$	$a$	$e$

## Group of Order 3

 $(\{e, a, b\}, *)$ 

$*$	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$b$	$e$
$b$	$b$	$e$	$a$

## Group of Order 1

 $(\{e\}, *)$ 

$*$	$e$
$e$	$e$

## Group of Order 2

 $(\{e, a\}, *)$ 

$*$	$e$	$a$
$e$	$e$	$a$
$a$	$a$	$e$

## Group of Order 3

 $(\{e, a, b\}, *)$ 

$*$	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$b$	$e$
$b$	$b$	$e$	$a$

## Group of Order 4

$*$	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

$*$	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$b$	$c$	$e$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$e$	$a$	$b$

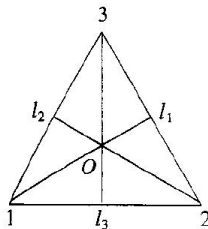
$*$	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$a$	$e$
$c$	$c$	$b$	$e$	$a$

$*$	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$c$	$e$	$b$
$b$	$b$	$e$	$c$	$a$
$c$	$c$	$b$	$a$	$e$



## Problem Description

- Given the equilateral triangle with vertices 1, 2, and 3. Consider its symmetries.
  - Rotation about the triangle center
  - Reflection about the angle bisector



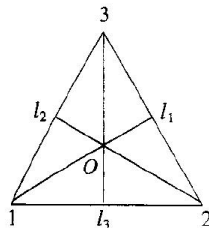
## Definition (Symmetries of the Triangle)

- Three counter-clockwise rotations  $f_1, f_2, f_3$  of the triangle about  $O$  through  $0^\circ, 120^\circ, 240^\circ$ , respectively.

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

- Three reflections  $g_1, g_2, g_3$  of the triangle about the lines  $l_1, l_2, l_3$ , respectively.

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$



## Theorem

♪  $(S_3, *)$  is a group, where

♪  $S_3 = \{f_1, f_2, f_3, g_1, g_2, g_3\}$

♪ the operation  $*$ , *followed by*, on the set  $S_3$  is defined as follows:

$*$	$f_1$	$f_2$	$f_3$	$g_1$	$g_2$	$g_3$
$f_1$	$f_1$	$f_2$	$f_3$	$g_1$	$g_2$	$g_3$
$f_2$	$f_2$	$f_3$	$f_1$	$g_3$	$g_1$	$g_2$
$f_3$	$f_3$	$f_1$	$f_2$	$g_2$	$g_3$	$g_1$
$g_1$	$g_1$	$g_2$	$g_3$	$f_1$	$f_2$	$f_3$
$g_2$	$g_2$	$g_3$	$g_1$	$f_3$	$f_1$	$f_2$
$g_3$	$g_3$	$g_1$	$g_2$	$f_2$	$f_3$	$f_1$

Compute  $f_2 * g_2$  Algebraically

♪ To compute  $f_2 * g_2$  algebraically, we compute  $f_2 \circ g_2$

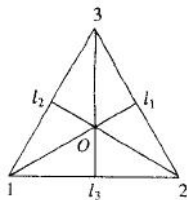
$$f_2 \circ g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = g_1$$

♪ Therefore

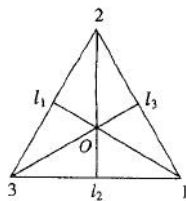
$$f_2 * g_2 = g_1$$

## Compute $f_2 * g_2$ Geometrically

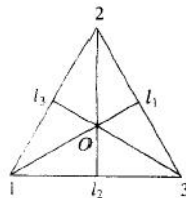
- ♪ We can also compute  $f_2 * g_2$  geometrically by rotating or flipping the triangle.



Given triangle



Triangle resulting after  
applying  $f_2$



Triangle resulting after applying  
 $g_2$  to the triangle at the left

## Definition (Permutation Group)

- ♪ The set of all permutations of  $n$  elements is a group of order  $n!$  under the operation of composition.
  - ♪ called the symmetric group on  $n$  letters, denoted by  $S_n$ .
  - ♪ permutation group: a group with some permutations of  $n$  elements

## Theorem (Cayley's Group Theorem)

- ♪ *Every Finite Group of order  $n$  can be represented as a Permutation Group on  $n$  letters.*

## Example

### ♪ A Cyclic Group

*	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>e</i>	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	<i>a</i>	<i>b</i>	<i>c</i>	<i>e</i>
<i>b</i>	<i>b</i>	<i>c</i>	<i>e</i>	<i>a</i>
<i>c</i>	<i>c</i>	<i>e</i>	<i>a</i>	<i>b</i>

## Definition (Cyclic Group)

♪ Check the Table on the left, we have

$$♪ a^0 = e$$

$$♪ a^1 = a$$

$$♪ a^2 = b$$

$$♪ a^3 = c$$

♪ Such a group is called a cyclic group.

## Homework

- ♪ 20,28 @page 323-324
- ♪ 12,16 @page 348
- ① Let  $G$  be a group. For  $a, b \in G$ , we say that  $b$  is conjugate to  $a$ , written  $b \sim a$ , if there exists  $g \in G$  such that  $b = gag^{-1}$ . Show that  $\sim$  is an equivalence relation on  $G$ . The equivalence classes of  $\sim$  are called the conjugacy classes of  $G$ .
- ② Let  $G$  be a group, and suppose that  $a$  and  $b$  are any elements of  $G$ . Show that if  $(ab)^2 = a^2b^2$ , then  $ba = ab$ .
- ③ Let  $G = \{x \in \mathbb{R} | x > 1\}$  be the set of all real numbers greater than 1. For  $x, y \in G$ , define  $x * y = xy - x - y + 2$ . Show that  $(G, *)$  is a group.