

Notes for M.A. Armstrong's *Groups and Symmetry*

Christian Stigen Larsen

March 2016

1 Symmetries of the Tetrahedron

Symmetry group Captures the rules of how symmetries combine for a given object.

Order of operations In the *product** xyz , do z first, then y and finally x . If order doesn't matter in G , it's commutative (or *abelian*). Remember to label geometric vertices.

Multiplication

- For $\mathbb{Q} - \{0\}$, \mathbb{Q}^{pos} , $\mathbb{R} - \{0\}$, \mathbb{R}^{pos} , $\{+1, -1\}$, $\mathbb{C} - \{0\}$, \mathbb{C}^\dagger , $\{\pm 1, \pm i\}$: $e = 1$ and $x^{-1} = 1/x$.

\mathbb{Z} under addition modulus n $e = 0$, $x^{-1} = n - x$ for $x \neq 0$, finite *abelian* group and denoted \mathbb{Z}_n .

\mathbb{Z} under multiplication modulus n Requires n to be prime.

2 Axioms

Group Set G with *multiplication* (addition, rotation, etc.) satisfying

- **associativity**, i.e. $(xy)z = x(yz)$
- **identity element** $e \in G$ such that $xe = x = ex$
- **inverse** $e \in G$ such that $x^{-1}x = e = xx^{-1}$

Properties common to all groups

- The identity element of a group is unique.
- The inverse of each element of a group is unique.

3 Numbers

Addition of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

- Identity is zero
- $-x$ is the inverse

*Rotations, flips, multiplications, additions, etc. Same order as functional composition.

4 Dihedral Groups

When $n \geq 3$ we can manufacture a plate which has n equal sides. These are the non-commutative *dihedral rotational symmetry groups* D_n . E.g. $D_3 = \{e, r, r^2, s, rs, r^2s\}$. $x^m x^n = x^{m+n}$ and $(x^m)^n = x^{mn}$ provided we interpret $x^0 = e$. For any multiplication table, each element in G appears only once in every given column or row.

$$r^n = e, s^2 = e, sr = r^{n-1}s, r^{n-1} = r^{-1}, \text{ etc.}$$

Each element is of form $r^a, r^a s$ where $0 \leq a \leq n-1$.

For $k = a +_n b$, $r^a r^b = r^k$ and $r^a (r^b s) = r^k s$. For $l = a +_n (n-b)$, $(r^a s) r^b = r^l s$ and $(r^a s)(r^b s) = r^l$ — thus r and s **generate** D_n .

The **order** $|G|$ is the number of elements in the group. If $x^n = e$, then the *element* x has *finite* order n when n is the smallest such n .

5 Subgroups and Generators

A **subgroup** of G is a subset of G which itself forms a group under the multiplication of G . For H to be a

[†]Complex numbers of modulus 1.

subgroup of G , $H < G$:

- $xy \in G$ for any $x, y \in H$
- $e_H \in G$
- For any $x \in H$, $x^{-1} \in G$
- Associativity in G implies the same for H .

Subgroup generated by x , or $\langle x \rangle$ For an element x in G , the set of all x^n is a subgroup of G (remember $x^0 = e$). Finite order m means $x^0 = e, x^1, \dots, x^{m-1}$. So order of $x \in G$ is precisely the order of $\langle x \rangle$. If $\langle x \rangle = G$, i.e., generates all of G , then G is a **cyclic group**.

Subgroup generated by X If $X < G^\ddagger$ and, for example, r, s, r^2, sr (called *words* of X).

Theorems

- A non-empty subset H of a group G is a subgroup of G if and only if xy^{-1} belongs to H whenever x and y belong to H .
- The intersection of two subgroups of a group is itself a subgroup.
- Every subgroup of \mathbb{Z} is cyclic. Every subgroup of a cyclic group is cyclic.

6 Permutations

A *permutation* is a bijection[§] from a set X to itself (e.g., replace all 3s with 1s). The collection of *all* permutations of X forms a group S_x under composition of functions (who each perform one specific permutation). When X consists of the first n positive integers, we get the **symmetric group** S_n of degree n and order $n!$. S_3 is not abelian

$(a_1 a_2 \dots a_k)$ is called a **cyclic permutation**, sending a_1 to a_2, \dots, a_k to a_1 . Its length is k and a cyclic permutation of length k is called a **k -cycle**. A 2-cycle is called a **transposition**. Every element of S_n can be written as many such **disjoint**, meaning no integer is moved by

[‡] X is a subgroup of G .

[§] A one-to-one mapping between the elements of two sets, meaning you can always go backwards as well.

more than one of them. Therefore they are *commutative*.

A few tricks

- Each *element* of S_n can be written as a product of cyclic permutations, and any cyclic permutation can be written as a product of transpositions: $(a_1 a_2 \dots a_k) = (a_1 a_k) \dots (a_1 a_3)(a_1)(a_2)$. Therefore, each *element* of S_n can be written as a product of transpositions.
- $(ab) = (1a)(1b)(1a)$
- $(1k) = (k-1, k) \dots (34)(23)(12)(23)(34) \dots (k-1, k)$

Theorems

- The transpositions in S_n together generate S_n .
- The transpositions $(12), (13), \dots, (1n)$ together generate S_n .
- The transpositions $(12), (23), \dots, (n-1, n)$ together generate S_n .
- The transposition (12) and the n -cycle $(12 \dots n)$ together generate S_n .

Any *element* α of S_n can be written as a product of *transpositions* in many different ways. But the number of transpositions is always even or always odd. If α can be written as the product of an even number of transpositions, then its sign must be $+1$; for odd, it is -1 . Therefore, by the first trick above, a *cyclic permutation* is even precisely when its length is odd.

Theorems

- The even permutations in S_n form a subgroup of order $n!/2$ called the **alternating group** A_n of degree n .
- For $n \geq 3$ the 3-cycles generate A_n .

7 Isomorphisms

If two multiplication tables have corresponding elements and products, they are **isomorphic**.

Theorem Two groups G and G' are *isomorphic* if there is a bijection ϕ from G to G' which satisfies $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$. The function ϕ is called an *isomorphism* between G and G' . This is written $G \cong G'$.

Notes

- G and G' have the same order.
- $\phi(x)^{-1} = \phi(x^{-1})$ for all $x \in G$.
- If G is abelian, then so is G' .
- If H is a subgroup of G then $\phi(H)$ a subgroup of G' .
- An isomorphism preserves the order of each element.
- If $\phi: G \rightarrow G'$ and $\psi: G' \rightarrow G''$ are both isomorphisms, then the composition $\psi\phi: G \rightarrow G''$ is also an isomorphism.