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.

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 identify 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.

Multiplication

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

4 Dihedral Groups

When $n \geqslant 3$ we can manufacture a plate whish 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.

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

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

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 $x^0 = e, x^1, \ldots, x^{m-1}$. 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 $X < G$[‡] and, for example, r,s,r^2,sr (called *words* of X).

Theorems

(5.1) 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.

(5.2) The intersection of two subgroups of a group is itself a subgroup.

(5.3) 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 collecticon 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

$(a_1 a_2 \ldots a_k)$ is called a ***cyclic permutation***, sending a_1 to a_2, ..., 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 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: $(a_1 a_2 \ldots a_k) = (a_1 a_k) \ldots (a_1 a_3)(a_1)(a_2)$. Therefore, each *element* of S_n can be written as a product of transpositions.
- $(ab) = (1a)(1b)(1a)$
- $(1k) = (k-1, k)\ldots(34)(23)(12)(23)(34)\ldots(k-1, k)$

Theorems

(6.1) The transpositions in S_n together generate S_n.

(6.2a) The transpositions $(12), (13), \ldots, (1n)$ together generate S_n.

(6.2b) The transpositions $(12), (23), \ldots, (n-1, n)$ together generate S_n.

(6.3) The transposition (12) and the n-cycle $(12 \ldots n)$ 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

(6.4) The even permutations in S_n form a subgroup of order $n!/2$ called the ***alternating group*** A_n of degree n.

(6.5) For $n \geqslant 3$ the 3-cycles generate A_n.

7 Isomorphisms

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

[‡] 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.

Two groups G and G' are ***isomorphic*** if there is a bijection φ from G to G' which satisfies $\varphi(xy) = \varphi(x)\varphi(y)$ 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.
- $\varphi(x)^{-1} = \varphi(x^{-1})$ for all $x \in G$.
- If G is abelian, then so is G'.
- If H is a subgroup of G then $\varphi(H)$ a subgroup of G'.
- An isomorphism preserves the order of each element.
- If $\varphi\colon G \to G'$ and $\psi\colon G' \to G''$ are both isomorphisms, then the composition $\psi\varphi\colon G \to G''$ is also an isomorphism.

Examples

- $\varphi\colon \mathbb{R} \to \mathbb{R}^{\textbf{pos}}$ by $\varphi(x) = e^x$ and $\varphi(x+y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y)$.
- The non-abelian, rotational group G for the tetrahedron is isomorphic to A_4.
- Any infinite cyclic group G is isomorphic to $\mathbb{Z}$ by $\varphi(x^m) = m$ and $\varphi(x^m x^n) = \varphi(x^{m+n}) = m + n = \varphi(x^m) + \varphi(x^n)$.
- Any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$ by $\varphi(x^m) = m \pmod{n}$.
- The numbers $1, -1, i, -i$ form a group under complex multiplication. It is cyclic, and i, $-i$ are both generators. It gives two isomorphisms between this group and $\mathbb{Z}_4$.
- D_3 and S_3 are isomorphic.
- There is no isomorphism between $\mathbb{Q}$ and $\mathbb{Q}^{\textbf{pos}}$.

8 Plato's Solids and Cayley's Theorem

Remember: A surjection between two finite sets which have the same number of elements must be a bijection.

- The rotational symmetry group of the tetrahedron is isomorphic to A_4.
- The cube and octehedron both have rotational symmetry groups which are isomorphic to S_4.
- The dodecahedron and icosahedron both have rotational symmetry groups which are isomorphic to A_5.
- If two solids are ***dual*** to one another, their rotational symmetry groups are isomorphic.

Theorems *Every* group is isomorphic to a subgroup of permutations:

(8.1) Cayley's Theorem. Let G be a group, then G is isomorphic to a subgroup of S_G.

(8.2) If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.

9 Matrix Groups

The set of all invertible $n \times n$ matrices with real numbers as entries forms a group under matrix multiplication: Matrix multiplication is associative, the $n \times n$ identity matrix $I_n = \epsilon$ and the inverse of AB is $B^{-1}A^{-1}$. This group is called the ***General Linear Group***, GL_n.

Matrix multiplication is not commutative for $n \geqslant 2$, so we have a family of *infinite non-abelian* groups GL_2, GL_3, etc. For $n = 1$ the single entry must be a non-zero number (the matrix is invertible), and reduces to ordinary multiplication of numbers. Hence, $GL_1 \cong \mathbb{R} - \{0\}$.

AB^{-1} is orthogonal and by theorem (5.1) the collection of all $n \times n$ orthogonal matrices is a subgroup of GL_n. This subgroup is called the ***Orthogonal Group***, O_n. Those elements of O_n which have determinant equal to $+1$ form a subgroup of O_n called the ***Special Orthogonal Group***, SO_n.

No further notes here, at the moment.

10 Products

The ***direct product*** $G \times H$ of two groups G and H is constructed by $(g, h)(g', h') = (gg', hh')$, where

$g, g' \in G$ and $h, h' \in H$. Thus, $(gg', hh') \in G \times H$ and $G \times H$ is a group. The correspondence $(g, h) \to (h, g)$ means that $G \times H$ is isomorphic to $H \times G$. Unless either of G or H are of infinite order, $|G \times H| = |G| \cdot |H|$. If both G and H are abelian, so is $G \times H$. In reverse, if $G \times H$ is abelian, so are both G and H.

E.g., the elements of $\mathbb{Z}_2 \times \mathbb{Z}_3$ are $\{0, 1\} \times \{0, 1, 2\} = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}$ and their elements are combined by $(x, y) + (x', y') = (x +_2 x', y +_3 y')$. We follow the convention of using $+$ for the group structure whenever we have products of cyclic groups. As continually adding $(1, 1)$ to itself, we can fill out the whole group, and therefore $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic and isomorphic to $\mathbb{Z}_6$.

Klein's group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is non-cyclic and isomorphic to the group of plane symmetries of a chessboard.

We write $\mathbb{R}^n$ for the direct product of n copies of $\mathbb{R}$.

Theorem (10.1) $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if the highest common factor of m and n is 1.

Theorem (10.2) If H and K are subgroups of G for which $HK = G$, if they have only the identity element in common, and if every element of H commutes with every element of K, then G is isomorphic to $H \times K$.

The linear transformation $f_J \colon \mathbb{R}^3 \to \mathbb{R}^3$ sends each vector $\boldsymbol{x}$ to $-\boldsymbol{x}$ and is called ***central inversion***.

Some important notions at the end of the chapter have been left out, currently.

11 Lagrange's Theorem

Let $H < G$ and break it up as the union of the $k + 1$ pieces $H, g_1 H, \ldots, g_k H$, then $|G| = (k + 1)|H|$.

(11.1) The order of a subgroup of a finite group is always a divisor of the order of the group.

Note: The opposite is not true; the existence of a divisor m of $|G|$ does *not* imply the existence of a subgroup of G.

Corrolaries

(11.2) The order of every element of G is a divisor of the order of G.

(11.3) If G has prime order, then G is cyclic.

(11.4) If x is an element of G then $x^{|G|} = e$.

(11.5) **Euler's Theorem.** If the highest common factor of x and n is 1, then $x^{\phi(n)}$ is congruent to 1 modulo n.

(11.6) **Fermat's Little Theorem.** If p is prime and if x is not a multiple of p, then x^{p-1} is congruent to 1 modulo p.

12 Partitions

Let X be a set and let $\mathscr{R}$ be a subset of the cartesian product $X \times X$. Given two points x and y of X, we say that x is ***related*** to y if the ordered pair (x, y) happen to lie in $\mathscr{R}$. If (a) each $x \in X$ is related to itself, (b) if x is related to y, then y is related to x, for any two points $x, y \in X$, (c) if x is related to y and if y is related to z, then x is related to z for any three points $x, y, z \in X$ — then we call $\mathscr{R}$ and ***equivalence relation*** on X. For each $x \in X$ the collection of all points which are related to it is written $\mathscr{R}(x)$ and called the ***equivalence class*** of x.

Theorems

(12.1) $\mathscr{R}(x) = \mathscr{R}(y)$ whenever $(x, y) \in \mathscr{R}$.