Summer of Science Report
Basics of Group Theory as a mathematical concept

Anuj Diwan
170070005

July 22, 2018

1 Introduction

Group theory is a branch of mathematics that deals with abstract objects known as groups, rings and fields which encompass essential properties of many well-known objects and sets from wide-ranging fields of mathematics, computer science, physics and chemistry. General results proved for groups can be specialized to prove non-intuitive and surprising theorems in quantum physics and quantum chemistry! They can also be used to solve the Rubik's cube.

The aim of this Summer of Science reading project is to extensively learn the theory behind groups. This report will describe, in brief, parts of group theory that I have learned so far. I hope the report will be useful as an overview of basic group theory.

2 Preliminaries

2.1 Binary Operations

1. Given a set S, a function $*$ defined $S \times S \to S$ is known as a binary operation on the set S. Here,$\times$ is the direct product. It is defined as follows:
   $G \times H = \{(g, h) \mid g \in G, h \in H\}$
   $*$ maps each ordered pair (s_1, s_2) of S to an element of S, denoted as $s_1 * s_2$.

2. This operation can be

   (a) Commutative: $a * b = b * a$ $\quad \forall a, b \in S$

   (b) Associative: $a * (b * c) = (a * b) * c$ $\quad \forall a, b, c \in S$

3. There is no relation between commutativity and associativity. There are examples of operations being commutative and associative, only commutative or only associative and neither commutative nor associative.

4. Examples include integer addition, real number multiplication, matrix multiplication, symmetric difference Δ of two sets, etc. One can already see the benefits of thinking about an abstract binary operation $*$ on an abstract set S and using results for ordinary entities like integers, matrices, and vectors.

2.2 Number Theory

1. **Division Algorithm:**
   If $a, b \in \mathbb{Z}$ and $b \neq 0$ one can write

   $$a = qb + r \text{ where } q \in \mathbb{Z} \text{ and } 0 \leq r < |b|$$

   Here a is the dividend, b the divisor, q the quotient and r the remainder. Here q and r are obtained *uniquely*.

2. In the above, if $r = 0$, then b is said to divide a, denoted $b \mid a$

3. **GCD and LCM**:

   (a) If $m, n \in \mathbb{Z}$ and at least one of them is non-zero, the largest positive integer x such that $x \mid m$ and $x \mid n$ is called the *Greatest Common Divisor* of m and n, denoted (m, n). We can use Euclid's algorithm [2] to obtain this GCD.

   (b) If $m, n \in Z$ and $m, n \neq 0$, then the smallest positive common multiple of m and n is called the *Least Common Multiple* of m and n, denoted $lcm(m, n)$. If $m = 0$ or $n = 0$ or $m = n = 0$, we can define $lcm(m, n) = 0$.

.

3 Groups-Introduction

- Given a set G and a binary operation $*$ (defined in 2.1), one calls the pair $(G, *)$ i.e one calls the set G **under the operation** $*$ a *group* if:

  1. $*$ is associative.
  2. There exists a special element $e \in G$, called an identity element, with the property

     $$e * g = g * e = g \quad \forall g \in G$$

  3. For each $g \in G$ there exists an element $g^{-1} \in G$, called the inverse of g such that

     $$g * g^{-1} = g^{-1} * g = e$$

     where e is the identity element from before.

  Clearly G must be a non-empty set.

- One can show that it follows from this definition of a group that there is a unique identity element e and a unique inverse for each element in G, thus allowing one to call it *the* identity and *the* inverse.

- One can also show that the existence of a right inverse and a right identity, or a left inverse and a left identity, is sufficient to show that G is a group. Existence of a right identity means existence of $e \in G$ such that $g * e = g \quad \forall g \in G$ and existence of a right inverse means existence of $g^{-1} \in G$ for each $g \in G$ such that $g * g^{-1} = e$. Similarly for left identity and left inverse.

- If $*$ is commutative, G is called an abelian group. The set

$$Z = \{z \in G \mid z * x = x * z \quad \forall x \in G\}$$

  is called the center of G. Thus for an abelian group $Z = G$.

- $(g^{-1})^{-1} = g$ and $(x * y)^{-1} = y^{-1} * x^{-1}$

- When the operation $*$ is non-abelian it is usually called multiplication and when it is abelian it is usually called addition. When referring to 'adddition', we may refer to $*$ as $+$ and g^{-1} as $-g$. We can also call $x^n = nx$. (What x^n is is explained in the next section.)

4 Cyclic Groups

- Since $*$ is associative, one can do away with writing parentheses when multiple variables are involved. Thus

$$abcd = (ab)(cd) = (a(bc))d \text{ and so on}$$

  Similarly, we can write, for brevity (here $n > 0$):

  1. $x^n = \underbrace{x * x * ... * x}_{\text{n times}}$
  2. $x^{-n} = (x^{-1})^n$
  3. $x^0 = e$

  Other obvious results like $x^{mn} = (x^m)^n$ follow directly.

- One of the most important things one can define for an element of a group is the order of the element.
  Given $x \in G$, if there exists a positive integer n such that $x^n = e$, the smallest such n is called the order of x, denoted by $o(x)$. If no such n exists i.e $x^n \neq e \quad \forall n \in \mathbb{Z}^+$ then $o(x) = \infty$.

- This quantity, $o(x)$ is very useful when we speak of cyclic groups.
  A group G is cyclic if all its elements can be expressed as integer powers of an element of G, called a generator of G i.e. if $x \in G$ and

$$G = \{x^n \mid n \in \mathbb{Z}\}$$

then $G = \langle x \rangle$ and x is called a generator of G. G may have more than one generator. Precisely how many generators it has is also known and will be explained soon. Clearly a cyclic group must be abelian, too.

- If $G = \langle x \rangle$ and $o(x) = \infty$, all elements of G must be distinct, because if two elements x^j and x^k are equal ($j \neq k$) and WLOG $j > k$ then $x^{(j-k)} = e$, contradicting $o(x) = \infty$. Similarly if $G = \langle x \rangle$ and $o(x) = n$ then G has n elements given by the powers of x from 0 to $n - 1$.

- Some results for orders:

  1. $o(x) = o(x^{-1})$
  2. If $x^n = e$, then $o(x) \mid n$.
  3. $o(x^m) = \dfrac{o(x)}{gcd(o(x), m)}$

  Refer to 2.2 for definition of | and GCD.

5 Subgroups

- The definition of a subgroup is straightforward and intuitive.
  A subset H of a group $(G, *)$ is called a subgroup if $(H, *)$ is a group i.e H forms a group under the operation $*$.
  Note that the subgroup needs to have the same operation as the parent group.

- The identity element of G and the identity element of H are the same.

- If H is a non-empty subset of G, H being a subgroup is equivalent to H being closed under multiplication (i.e closed under $*$) and being closed under inverses.

  1. Closed under multiplication: If $a, b \in H$, then $a * b \in H$
  2. Closed under inverses: If $a \in H$, then $a^{-1} \in H$ where a^{-1} refers to the inverse of a in the group $(G, *)$.

- The proofs of some of the results that follow are slightly lengthy and therefore will be omitted. Only a short intuitive explanation will be given. All the proofs are available in the textbook.

- If a group is cyclic, all of its subgroups are cyclic. In particular, if $G = \langle x \rangle$, then for any subgroup H, $H = \langle x^n \rangle$ where n is the smallest positive integer n satisfying $x^n \in H$.
  It is immediate that $\langle x \rangle$ where $x \in G$ is a subgroup of G. Thus if G is cyclic, the groups generated from each of its elements are all the possible subgroups of G. Clearly, not all these groups are distinct.

- Let $G = \langle x \rangle$ be a cyclic group of finite order n. Then:

1. G has a subgroup of order $m \iff m \mid n$
2. $m \mid n \implies G$ has a unique subgroup of order m, generated by $x^{\frac{n}{m}}$.
3. $\langle x^r \rangle = \langle x^s \rangle \iff (r, n) = (s, n)$

Refer to 2.2 for definition of $\mid$ and (m, n), the GCD.

- This shows that since $G = \langle x \rangle$ and $(1, n) = 1$, $G = \langle x^r \rangle$ if and only if $(r, n) = 1$. Since $0 \leq r < n$, the number of distinct generators of G is equal to the number of non-negative integers less than n and co-prime to n. This number is called $\phi(x)$, Euler's totient function.
  We also see that the number of distinct subgroups of G is equal to the number of positive divisors of n. Each distinct subgroup is generated x^r, where r is a distinct positive divisor of n.

- We can see that if J, K are subgroups of a group G, then their intersection $J \cap K$ is also a subgroup. Slightly less obvious is the fact that $J \cup K$ is a subgroup only if one of them is entirely contained within the other.
  $J \cup K$ is always closed under inverses, but will fail to be closed under multiplication if the above condition is not satisfied. If we take one element from J that is not in K and an element from K that is not in J and multiply them, the resulting element will neither be in J nor in K.

6 Direct Products

- We can *combine* two or more groups to make a new group. This can be done for example using the direct product. Let $(G, *_g)$ and $(H, *_h)$ be two (not necessarily distinct) groups. We can define a new set $G \times H$ where $\times$ is the usual direct product on two sets (see 2.1) and define a binary operation $*$ on $G \times H$ as follows:
  If $v_1 = (g_1, h_1) \in G \times H$ and $v_2 = (g_2, h_2) \in G \times H$, then

$$v_1 * v_2 = (g_1, h_1) * (g_2, h_2) = (g_1 *_g g_2, h_1 *_h h_2)$$

- Analogously we can combine n groups using $\times$. In fact infinitely many groups can also be combined using the direct product but this is rarely done.

- Let $G = G_1 \times G_2 \times ... \times G_n$. Then

  1. Let $g_i \in G_i$ for each i from 1 to n, and let each g_i be of finite order. Then, $o((g_1, g_2, ..., g_n)) = lcm(o(g_1), o(g_2), ..., o(g_n))$
  2. Suppose each G_i is cyclic and of finite order. Then:
     G is cyclic $\iff gcd(|G_i|, |G_j|) = 1$ for $i \neq j$

7 Functions

- The precise definition of a mapping(not a function) is as one expects it to be:
  A *mapping* f from a set S to a set T is a set consisting of ordered pairs (s,t) where $s \in S$ and $t \in T$.
  Usually one prefers that this set be non-empty, but the mathematical definition does not impose this upon it.

- A *function* $f : S \to T$ is a mapping with an additional property:
  $\forall s \in S, \exists$ exactly one $t \in T$ such that $(s,t) \in f$.
  Informally a function assigns one element to each element in S.

- A few standard definitions:

  1. f is called injective(or one-to-one) iff for all $s_1, s_2 \in S$, $f(s_1) = f(s_2) \Leftrightarrow s_1 = s_2$.
  2. f is called surjective(or onto) iff for all $t \in T$, there exists an $s \in S$ such that $f(s) = t$.
  3. f is called bijective iff it is both injective and surjective.

- Consider the formal definition of a mapping, or of a function. If we reverse the order of the elements in the pairs (s,t), we obtain the *inverse mapping* f^{-1} from T to S. If f is a function, f^{-1} is a function only if f is bijective. This can be easily proved. Here f^{-1} is also bijective. It is apt to refer to it as the inverse, as one shall see below.

- Consider two functions of the form $f : S \to T$ and $g : T \to U$. We can define a binary operation called *composition* i.e $\circ$, that outputs a function of the form $g \circ f : S \to U$ on two functions of this form. We define $g \circ f\ (s) = g(f(s)) \forall s \in S$. This is a valid definition of a mapping because $f(s) \in T$ and g expects values from T. This is a function because if s maps to exactly one value in T, $f(s)$, and $f(s)$ maps to exactly one value in U, $g(f(s))$, then s maps to exactly one value in U, $g(f(s))$.

- Let $i_S : S \to S$ such that $\forall s \in S, i_S(s) = s$ and $i_T : T \to T$ such that $\forall t \in T, i_T(t) = t$. Then, $f^{-1} \circ f = i_S$ and $f \circ f^{-1} = i_T$. i_S and i_T are called identity functions.

- We shall now introduce group theory into all the ideas of inverses, compositions and identity functions. The terminology itself heavily hints to what one constructs next.
  Let X be a non-empty set and let S_X be the set of all bijective(see point 3) functions from X to X. Then, one claims that:
  $(S_X, \circ)$ is a group. A bijective function from X to itself is known as a permutation of X and this group is called the *symmetric* group on X.

- Proof: First, $\circ$ is a valid binary operation on S_X because if f and g are bijective then $f \circ g$ is bijective, because if $f(g(s_1)) = f(g(s_2))$, then $g(s_1) = g(s_2)$ and hence $s_1 = s_2$ since f and g are bijective. Surjectivity is also easily shown. Next, we can show associativity of $\circ$ using associativity of nested functions. Next, we claim i_X(the identity mapping on X) is the identity element, which is trivial. And finally we can use our previous result(point 7) to show that the (functional) inverse of f, f^{-1}, is the (group theoretic) inverse of f.

8 Symmetric groups

- Refer to point 5 in section 9 for the definition of the symmetric group of order n. We currently discuss symmetric groups on finite sets only. Let us denote $\{1, 2, \ldots, \}$ by X and its symmetric group by S_n. The identity element is i_n.

- All members of S_n can be expressed in a more compact way using special members of S_n called cycles, defined as follows:
  An r-cycle, denoted by $(x_1, x_2, \ldots, x_r)$ where $r \geq 1$ and each $x_i, 1 \leq i \leq r$ is a distinct element of X, is defined as the permutation f such that if $r = 1$, $f = i_n$ and if $r \geq 2$, $f(x_j) = x_{j+1}$ for $1 \leq j \leq r-1$, $f(x_r) = x_1$, and all other elements map to themselves. One can clearly see that by cyclically permuting x_1 through x_r one can get different representations of the same cycle.

- Two cycles A,B are called disjoint if no element is moved by both cycles i.e. $\nexists\ x \in X$ such that $A(x) \neq x$ and $B(x) \neq x$. Disjoint cycles commute under the $\circ$ operation.

- One can state a theorem similar to the Fundamental Theorem of Algebra(unique prime factorization theorem) for cycles:
  Every permutation can be expressed as a $\circ$ product of disjoint cycles i.e for every $\sigma \in S_n$, there exist disjoint cycles $f_1, f_2, ..., f_m$ such that $\sigma = f_1 \circ f_2 \circ \ldots \circ f_m$. Moreover, if one excludes $1-$cycles and ignores reordering of elements within cycles and commuting the cycles amongst themselves, one can obtain these m cycles uniquely. This is called cycle decomposition. m can possibly be 0, as is the case for the cycle decomposition of the identity permutation.

- The proof of the uniqueness of this decomposition is hard and is omitted. The proof of the existence of such m cycles is straightforward. For the permutation σ, consider the element 1 of X and call it x_1. Consider $x_2 = \sigma(x_1), x_3 = \sigma(x_2)$ and so on. Since X is finite, the must be some index k for which x_k equals some previous element, say x_j. Let x_k be the first such element, i.e. k is the smallest such number. Then, j must be 1, because if it is not, $x_{k-1} = x_{j-1}$ which contradicts the assumption that k is the smallest such number. Further, this implies that the elements $x_1, x_2, \ldots, x_{k-1}$ are distinct. Thus $c_1 = (x_1, x_2, ..., x_k)$ is a cycle that permutes a non-zero subset of X. Write $\sigma = c_1 \circ h_1$ where h_1 permutes all the elements of X excluding the x_is. h_1 permutes some number of elements, where this number is at least one less than n. If h_1 is the identity, we are done. Else, we apply the same idea on any element y_1 moved by h_1. h_1 does not move any of the x_is and hence when it is applied on y_1 any number of times, it never equals any of the x_is by the bijectivity of σ. Thus, h_1 contains a cycle c_2 consisting of elements not contained in c_1. Thus $\sigma = c_1 \circ c_2 \circ h_2$ where h_2 moves elements that are neither in c_1 nor c_2. The cardinality of the set of elements that each subsequent h_k moves strictly decreases with each k and since X is finite, at some k, there is nothing left to move and we are done.

- The previous proof is heavy and it helps to take a second look to understand it fully. $2-$cycles are called *transpositions*. This definition of course makes sense when X has at least 2 elements. Clearly the inverse of a transposition is itself. If $n \geq 2$, then the

$n-$cycle can be written as a product of transpositions as follows:
$(x_1, x_2, \ldots, x_n) = (x_1, x_n) \circ (x_1, x_{n-1}) \circ \ldots \circ (x_1, x_2)$ or
$(x_1, x_2, \ldots, x_n) = (x_1, x_2) \circ (x_2, x_3) \circ \ldots \circ (x_{n-1}, x_n)$

- In fact there are numerous different ways to write a cycle as a product of transpositions. Thus, the uniqueness of factorization has been lost. Using 8 and 8, we thus see that any permutation can be written as a product of transpositions. The following theorem is interesting(won't be proved):
  If we express $\sigma \in S_n$ as a product of s disjoint cycles $c_1, c_2, \ldots, c_s$ such that each element of X appears in some cycle, then the minimum number of transpositions required to create σ is $n - s$. Note that our definition of the s cycles may require $1-$cycles to make each element of X appear in some cycle.

- A permutation is called *even* if it can be written as a product of even number of transpositions, and is called *odd* if it can be written as product of odd number of transpositions. As we expect, a permutation can be either odd or even, not both.

- The above statement's proof is as follows. Suppose a permutation is both even and odd. Write it as $\sigma = x_1 x_2 \ldots x_t = y_1 y_2 \ldots y_s$ where t is even and s is odd. Then taking the RHS over to the LHS using inverses and using the fact that the inverse of any transposition is itself and because $t + s$ is odd, we get that the product of an odd number of transpositions equals the identity permutation. To disprove this, we shall consider the following statement about any permutation σ expressible as a product of m transpositions, $t_1 \circ t_2 \circ \ldots \circ t_m$.
  Either

  1. σ is not the identity permutation, or
  2. σ is expressible as the product of $m - 2$ transpositions.

  To prove it, consider any element a from $X = \{1, 2, \ldots, n\}$ that appears in some t_i, and let WLOG $t_j = (a, b)$ be the first such t_i from the right. If $j \neq 1$, we are done as a then appears exactly once considering all the transpositions, and thus σ definitely maps a to b and not to itself, hence σ cannot be the identity. If j is not 1, we can consider t_{j-1}. We can consider 4 cases for this: it is

  1. (a, b)
  2. (a, c) $c \neq b$
  3. (b, c) $c \neq a$
  4. (c, d) $c, d \neq a, b$.

  If the first, we delete $t_{j-1} t_j$ and we are done as σ is expressible as the product of $m - 2$ transpositions. For the other three,

  2. $(a, c) \circ (a, b) = (a, b) \circ (b, c)$
  3. $(b, c) \circ (a, b) = (a, c) \circ (b, c)$

4. $(c,d) \circ (a,b) = (a,b) \circ (c,d)$

In each of the three cases, we have managed to obtain an equivalent expression for σ in which the first occurrence of a from the right is one transposition further left than earlier. Repeating the argument, either the first case occurs and we obtain that σ is expressible as the product of $m-2$ transpositions, or we eventually reach t_1 and then we obtain that σ is not the identity.
Now, suppose the identity can be expressible as the product of an odd number of transpositions, say m number of transpositions. Then it can be expressed as the product of $m-2$ number of transpositions, and so on, till we reach 1. Clearly just one transposition moves two elements and hence cannot be the identity. Thus we are done.

- For $X = \{1, 2, \ldots, n\} n \geq 2$, consider the subset of S_n consisting of all even permutations. This is a subgroup, because the product of two even permutations is even, and the inverse of an even permutation $t_1 \circ t_2 \circ \ldots \circ t_k$ is $t_k \circ t_{k-1} \circ \ldots \circ t_1$ and hence even. This subgroup is called the alternating subgroup of degree n, A_n. We can easily see $|S_n| = n!$ and the number of even and odd permutations is equal, as left multiplication by (1,2) gives an odd permutation from an even one and an even one from an odd one.

- It is interesting to note that $(S_3, \circ)$ is non-abelian, and it is provable that all groups with ≤ 5 elements are abelian, hence S_3 is a smallest non-abelian group. The process of keeping a cardboard with vertices labelled $1, 2, 3, 4$ on a square drawn on the floor with vertices labelled $1, 2, 3, 4$ and considering which vertex of the square coincides with which vertex of the cardboard as a permutation of $\{1, 2, 3, 4\}$ gives rise to a correspondence between the elements of S_4 and physical *symmetry* operations like rotation, reflection(flipping), etc. of the cardboard.

9 Important groups

1. $GL(n, F)$ is the group of the set of $n \times n$ invertible matrices on F under matrix multiplication
where $n \in \mathbb{Z}^+$ and $F = \mathbb{R}$ or $\mathbb{C}$ or $\mathbb{Z}$ or in general any field or ring

2. $SL(n, F)$ is a subgroup of $GL(n, F)$ consisting of matrices with determinant 1

3. $(\mathbb{Z}_n, \oplus)$ is the set $\{0, 1, 2, ..., n-1\}$ under modulo addition i.e $a \oplus b$ is the remainder(from the Division Algorithm) when $a + b$ is divided by n.

4. V or K_4 is the Klein 4-group. Here
$$V = \{e, a, b, c\}$$
where $*$ is abelian, $ea = a, eb = b, ec = c, a^2 = b^2 = c^2 = e, ab = c, bc = a, ca = b$.

5. S_n is the symmetric group of degree n. S_n is the symmetric group on the set $X = \{1, 2, \ldots, n\}$. Here $1, 2, \ldots, n$ are not necessarily natural numbers but instead are symbols used to represent the elements of any set of cardinality n.

6. Alternating subgroup of degree n, A_n, as defined in point 8 of section 8.

References

[1] Dan Saracino. *Abstract Algebra: A First Course, Second Edition*. Waveland Press, 2008.

[2] greenfie@math.rutgers.edu:
`http://sites.math.rutgers.edu/~greenfie/gs2004/euclid.html`