# Notes on Group Theory:

## *Rubik's Cube and the Permutation Group*

Coding Club

September 23, 2024

Mohammed Alshamsi
2021004826
mo.alshamsi@aurak.ac.ae


Department of Computer Science and Engineering
American University of Ras Al Khaimah
2023–24

# Contents

# 1 Introduction

Welcome to the third set of "lecture notes" for the AURAK Coding Club. The idea is to introduce a useful topic that lends itself easily to coding applications. These topics tend to be mathematical in nature, but most (if not all) of it will be intuitive material that doesn't require much background knowledge.

## 1.1 How to Read this Document

This is essentially just a short monologue about group theory and related concepts. We'll go over the elementary definitions and results, and give some examples. This is by no means meant to give you a comprehensive introduction; it's just a quick tour to get you started. Check the bibliography if you want to learn more about the topic.

I'll be sure to bring up coding aplications whenever it makes sense. Any code I write at those points will be in the C language. If you've taken (or are taking) CSCI 112, you'll be able to follow along without much trouble. Furthermore, there will be coding exercises. You're free to solve them in any language.

If you don't know any coding, check this link for a quick intro to C.

## 1.2 Sets

Briefly, a group is a set that has some additional structure, so the following few subsections will review sets and introduce a few related concepts that will be helpful later. Feel free to skim this section to confirm what you (don't?) know.

**Sets.** The concept of a "set" is no doubt very familiar to you, at least intuitively. It's simply a collection of things—a collection that is *well-defined* in the sense that it's always clear whether a given object is (or is not) a part of that collection.

Sets are denoted by curly braces $\{\}$, with their *elements* (the "things" in them) being contained between the braces and separated by commas. For instance,

$$S = \{a, b, c\}$$

is a set consisting of the elements $a$, $b$ and $c$.

The set $S$ was defined *explicitly*. This means its constituent elements were all listed. If you were presented with $c$, for example, you would very easily be able to say that "$c$ is an element of $S$", or "$c \in S$", for short. Had you been presented with $d$, you would also be able to say that "$d$ is not an element of $S$", or "$d \notin S$".

You could also define sets implicitly, by defining a "property" that is held by the elements of that set, and by nothing else:

$$\{x \mid x \text{ is a member of the AURAK coding club's management as of September 23, 2024.}\}$$

This reads as "The set of all $x$, where $x$ is a [...]". Of course, descriptions like this need additional context that should be provided by the reader's knowledge.

Another way to implicitly define sets is by using the "..." notation, for instance

$$S = \{1, \ldots, 16\}.$$

But this, too, may rely on the reader's knowledge (or even be vague, leaving it to the reader to guess the right "rule" to identify the set by). For example, is $S$ the set of positive integers between 1 and 16 inclusive, or perhaps the set $\{1, 2, 4, 8, 16\}$ of the first five nonnegative powers of 2? Or the set $\{1, 4, 16\}$ of powers of 4?

**Subsets.** Given two sets $S$ and $T$, we say that $T$ is a *subset* of $T$ if every element of $T$ is in $S$. This is denoted by $T \subseteq S$, and if $T$ is not a subset of $S$ (meaning it contains elements that are outside of $S$), we denote that by $T \not\subseteq S$. Here we list all the subsets of $S$:

$$\{\} \qquad \{a\} \qquad \{b\} \qquad \{c\}$$
$$\{a, b\} \qquad \{a, c\} \qquad \{b, c\} \qquad \{a, b, c\}$$

Note that $S$ itself is also there; every set is a subset of itself. Also note the presence of the empty set $\{\}$, which is usually denoted by $\emptyset$. This set contains nothing, but is a subset of every other set.

**Exercise 1.** For a set of $n$ elements, how many subsets does it have?

**Exercise 2.** Is the empty set a subset of itself?

**Operations on sets.** There's three primary operations that involve sets:

1. $A - B$ is the set of all elements of $A$ that are not in $B$. This may also be denoted $A \setminus B$, and is named the *difference* of $A$ and $B$[1]or the *relative complement* of $B$ in $A$.

   You may also use this to subtract individual elements from a set. Knowing that $\mathbb{Z}$ is the set of all integers, $\mathbb{Z} - \{2\}$ is the set of all integers I don't like.

2. $A \cap B$ is the *intersection* of $A$ and $B$, and is the set of all elements of $A$ that are also in $B$ (or vice versa; it's the same thing).

3. $A \cup B$ is the *union* of $A$ and $B$, and is the set of all elements of $A$ and all elements of $B$.

## 1.3 Functions

Next, we build up to the fundamental notion of a function.

**Cartesian products.** An important property of sets is that "order doesn't matter". For a quick example, the sets $\{a, b\}$ and $\{b, a\}$ are equal. So, how do we express the notion of order?

There's a different notation for this, which is $(a, b)$, and is called an *ordered couple*, or an *ordered pair*. It establishes $a$ as the "first" element, and $b$ as the "second" element.[2] We may

[1]Yes, this may be vague in that it may mean $A - B$ or $B - A$.

[2]This can actually be defined in terms of sets, too. An example is

$$\{\{a\}, \{a, b\}\}.$$

There are other methods as well.

also have ordered triples, 4-tuples, or in general $n$-tuples for any natural number $n$, following the same notion of having a first, second, third, ...element. If we don't want to emphasize that $n$ is a specific number, we may also simply say "tuple".

The cartesian products of two sets $X$ and $Y$ is denoted $X \times Y$, and refers to the set of all ordered pairs $(x, y)$ where $x \in X$ and $y \in Y$. A good example is the $xy$-plane you're familiar with; it's the cartesian product of the set of real numbers $\mathbb{R}$ with itself. In cases like that, there's a notational shortcut that tends to be used: $\mathbb{R}^2$ is the same as $\mathbb{R} \times \mathbb{R}$.

**Functions.** A *function* $f$ from a set $X$ to a set $Y$ is a "rule" that assigns to each element $x$ of $X$ exactly one element $f(x)$ of $Y$. $X$ is said to be the *domain* of the function, and $Y$ is said to be its *codomain*. This is summarized by the notation $f : X \to Y$. We call $f(x)$ the *value* of $f$ at $x$.

Functions act on single elements of sets, but these elements may be anything; even tuples. So we can do something like $f : X \times Y \to Z$, assigning for each pair $(x, y)$ in the domain $X \times Y$ an element of the codomain $Z$. Note that multiple elements of the domain can map to the same element of the codomain, but for a given element of the codomain, there is at most one element of the domain that maps to it. This means some elements of the codomain cannot be "reached" by the function; for instance, $f : \mathbb{Z} \to \mathbb{Z}$ where the rule is doubling (so 2 goes to 4). The codomain is $\mathbb{Z}$, but all the odd numbers have no elements mapping to them. We call the set of all "reachable" elements in the codomain the *range* of the function, or alternatively, its *image*.

We'll use the word "operation" often when discussing groups, so now is a good time to define them. An operation $*$ on a set $X$ is simply a function mapping $X \times X$ to $X$; that is, $* : X \times X \to X$. Keep in mind that they're just a type of function that occurs often enough to warrant having more convenient notation for them. In the case of operations, we don't write $*(x_1, x_2)$ to denote the value of $*$ at $(x_1, x_2)$—instead, we write $x_1 * x_2$.

There is an operation that can be done on functions, called function composition. Given two functions $f : X \to Y$ and $g : Y \to Z$, their composition $g \circ f$ is the function which maps $x \in X$ to $g(f(x)) \in Z$. In other words, you first apply $f(x)$, then apply $g$ on the result.

**Injective, Surjective, and Bijective Functions.** These are properties that functions may have. Functions that have these properties are respectively said to be injections, surjections, and bijections.

Injective functions are those where every element of the codomain is mapped to by *at most* one element of the domain. That is, with injective functions, you can't have two *distinct* elements of the domain that map to the same element of the codomain.

Surjective functions are those where every element of the codomain is mapped to by *at least* one element of the domain. Intuitively, is means that the entire codomain is "reachable" by the function, so we can restate surjectivity as the property of having the range/image of the function be the same as its codomain.

Bijective functions are those that are both surjective and bijective. Every element of the codomain is mapped to by *exactly* one element of the domain, and in fact, the opposite is true. There are two properties of bijective functions that are of considerable importance:

1. They are invertible. This means that given a bijection $f : X \to Y$, there exists a bijection denoted $f^{-1} : Y \to X$ such that $f \circ f^{-1}$ maps $y$ to itself, and $f^{-1} \circ f$ maps $x$ to itself. So if

you have $f(x)$ and want to obtain $x$, just apply $f^{-1}$. This function $f^{-1}$ is said to be the *inverse* of $f$. Of course, $f$ itself is $\left(f^{-1}\right)^{-1}$.

2. Sets with a bijection between them are said to have the same *cardinality*, which means they have the same number of elements. This is a very obvious fact when dealing with finite sets, but it's useful when reasoning about infinite sets. For example, you can prove that the set $\mathbb{R}$ is larger than $\mathbb{N}$ because no matter what function $f : \mathbb{N} \to \mathbb{R}$ you try to define, it's possible to show that there exists some element of $\mathbb{R}$ that isn't mapped to. This means the function is not surjective, and therefore not bijective. (Look up Cantor's diagonalization argument for more information on this.)

## 2 What is a Group?

Most of the information in the previous section will be relevant in some way, so if you're unclear on any of that, I suggest you go back and reread it, or find some resources online to help you understand it.

A group is an ordered pair of a set $G$ and an operation $*$ on $G$, satisfying the following:

1. **Associativity:** The operation $*$ must be associative. For any three elements $a$, $b$, and $c$ of $G$, $a * (b * c)$ must be equal to $(a * b) * c$.
2. **Identity:** There is an element $e$ in $G$, such that $e * a = a * e = a$ for all $a$ in $G$.
3. **Inverse:** For every element $a$ in $G$, there exists an element, denoted $a^{-1}$, such that $a * a^{-1} = a^{-1}a = e$.

You can refer to this group by the usual ordered pair notation, so $(G, *)$. But that's a little unwieldy, so usually we'll instead use $G$ to refer to the group. When we want to refer to the set—which is fairly rare—we'll say "the group set of $G$". Another notational shortcut we will make use of is omitting the operation symbol $*$; so instead of $a * b$ we'll often use $ab$ instead.

I list some familiar examples here. Take some time to compare these with the definition. I'll do the first two.

1. The set $\mathbb{Z}$ of all integers, under the operation of addition. We already know addition is associative. The identity of this group is $0$, because $0 + a = a + 0 = a$ for all integers $a$. Finally, the inverse of an integer $a$ is its negative; $a + (-a)$ gives you the identity of $0$ no matter what $a$ is.[3] This group is called the *additive group of integers*.
2. The set $\mathbb{Q}$ under addition.
3. The set $\mathbb{Q} - \{0\}$ under the operation of multiplication. (Consider also why $0$ can't be an element of this group.)

Here's a more interesting example. Consider the group of integers modulo $n$, where the set is

$$\{0, 1, \ldots, n-1\}$$

and the operation is addition modulo $n$. This operation goes as follows: add the two numbers normally, then find the remainder when dividing by $n$. (For example, the sum of 4 and 5 modulo

[3] Keep in mind that $a^{-1}$ isn't $\frac{1}{a}$ in this case; in fact, reciprocals aren't even a thing here since we're dealing with integers. What $a^{-1}$ means is heavily dependent on what the operation of the group is.

6 is 3, because the remainder of $9/6$ is 3.) The identity here is still 0, but the inverses now aren't negative numbers or reciprocals. Instead, we have that the inverse of 1 is 5, the inverse of 2 is 4, and so on. Notice that these pairs (apart from the pairing of 0 with itself) always add up to 6, which—when divided by 6—gives a remainder of 0, the identity. That's what makes them inverses.

Another example, which helps cement how general the concept of a group can be, is the group of invertible $n \times n$ matrices under matrix multiplication. If you've taken MATH 203 (or are decently familiar with matrices from high school), you know the following facts:

1. Matrix multiplication is associative; given three $n \times n$ matrices $A$, $B$, and $C$, the product $(AB)C$ is equal to $A(BC)$.
2. There is an identity matrix of size $n \times n$, denoted by $I_n$, that has 1s along the diagonal and 0s everywhere else. This has the property that $I_m A = A I_n = A$ for any $m \times n$ matrix $A$. Two identity matrices are
$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \text{and} \qquad I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$
3. Some matrices are invertible. The product $AB$ of two invertible matrices $A$ and $B$ is another invertible matrix, and its inverse is $B^{-1}A^{-1}$.

Notice that these three facts correspond to the definition of a group. So for each $n \geqslant 1$, we have a group composed of all the invertible matrices of size $n \times n$.

The third point deserves special mention, because this fact is true for *all* groups: for any two elements $a$ and $b$ of a group, the inverse of $ab$ is $b^{-1}a^{-1}$. The proof is simple:

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

Here's some rapid-fire of other basic properties that are true of every group. Feel free to take some time to prove some for yourself; the proofs are about as long as the above.

1. There is exactly one identity element in a group.
2. If $ab = ac$, then $b = c$, and if $ba = ca$, then $b = c$.
3. If $ab = e$, then $a = b^{-1}$ and $b = a^{-1}$.
4. The inverse of $a^{-1}$ is $a$ itself.
5. Each element has exactly one inverse.
6. If $a^2 = a$, then $a = e$.

**Cayley Tables.** These are a nice way to outline the structure of a (finite!) group. They're nice because they can actually tell you whether the group has specific properties. We'll see how with the following example, which is the Cayley table of the group of integers modulo 6 under addition.

| $+$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

From this table, you can see what the inverse of each element is, by observing the row and column of each individual 0 entry. The fact that the table is symmetric along the main diagonal tells you that the group's operation is *commutative*, which in general means that $ab = ba$ for all $a$ and $b$. A group with a commutative operation is called an *abelian group*. Finally, notice that no row or column contains two occurrences of the same element.[4] This is true of every group's Cayley table, in fact.

Next, let's look at the Cayley table of another group. Suppose we have the following matrices:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

$$C = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix} \qquad D = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \qquad K = \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix}$$

We get the following Cayley table for the group of these matrices under matrix multiplication.

| $\cdot$ | I | A | B | C | D | K |
|---|---|---|---|---|---|---|
| I | I | A | B | C | D | K |
| A | A | I | C | B | K | D |
| B | B | K | D | A | I | C |
| C | C | D | K | I | A | B |
| D | D | C | I | K | B | A |
| K | K | B | A | D | C | I |

Since this group isn't abelian, the order of operations is important to understand how to read the table. I've highlighted a row and column to illustrate: is the K here the result of $BA$, or $AB$? The answer is the former; the first element is that which labels the row.

## 2.1 Subgroups, Generators, and Cyclic Groups

In the previous section we discussed two examples of groups of matrices. The first example was a family of groups: the group of all invertible $1 \times 1$ matrices, the group of all invertible $2 \times 2$

[4] Look up Latin squares. They're pretty cool. Also see Graeco-Latin squares.

matrices, and so on. The second example was a finite group consisting of six $2 \times 2$ matrices. We can observe from these two examples that a group may contain another, smaller group.

Given a group G, if a subset of its elements form a group under the same operation, then the subset and operation are said to form a *subgroup* of G. It's important to note there is a sense of "closure" here, where applying the operation on any two elements of that subset also produces an element of the subset; and, the inverse of every element in the subset is also in the subset.

So we already saw one example with the six matrices. An example which is true for all groups is $\{e\}$; this is commonly referred to as the trivial subgroup. Try proving that this is a group. Another one—also true for all groups G—is G itself. When we want to say "a subgroup of G that isn't G itself", we say "a proper subgroup of G".

Here's another example. The group of integers modulo 12 has six subgroups, with sets $\{0\}$, $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$, $\{0, 2, 4, 6, 8, 10\}$, and $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. This enumeration by itself introduces us to several notions.

**Generating Sets.** Given a group G and a subset S of G's group set, the set of all possible combinations (under G's operation) of the elements of S and their inverses, forms a subgroup of G. S is said to be the generator of this subgroup, and the subgroup is denoted $\langle S \rangle$.

That's a mouthful, so let's break it down with a few examples.

1. The additive group of integers can be generated by the set $\{1\}$, because you can—in finitely many steps—produce any element of $\mathbb{Z}$ by repeatedly adding or subtracting 1. A proper subgroup of this group may be generated by any other element of $\mathbb{Z}$; for example, the set $\{2\}$ generates the group of all even integers under addition.
2. You can also generate $\mathbb{Z}$ using any pair of *coprime* numbers.[5]
3. The group of six matrices from the previous section has a subgroup $\langle\{B\}\rangle = \{I, B, D\}$, and another subgroup $\langle\{A\}\rangle = \{I, A\}$. The set $\{A, B\}$ generates the entire group $\{I, A, B, C, D, K\}$.
4. $\{2\}$ generates the group $\{0, 2, 4, 6, 8, 10\}$ under addition modulo 12. The same is true of $\{0\}$, $\{6\}$, $\{4\}$, $\{3\}$, and $\{1\}$ for the other subgroups we listed. $\{2, 3\}$, $\{3, 4\}$, and any subset containing 1 all generate the entire group.

There's one more example, but we'll cover it in Section 2.2.

### Cyclic Groups.

### Order.

We define generators and cyclic groups, as well as generating sets of not-necessarily-cyclic groups. We note that their ability to "generate" the group relies heavily on the operation in question.

[5] These are pairs of numbers that don't share any factors apart from 1. See the number theory notes for more information on this topic, including Bézout's identity, which makes it possible to generate $\mathbb{Z}$ in this way.

### 2.2 Groups of Permutations

Yeah these are pretty cool. We'll define groups of permutations, show the two slick notations, and maybe the algorithm(s?) from TAOCP S1.3.3. (The scope creep has already begun, but it won't be as bad as the whole string search algorithm from last time... hopefully.)

## 3 Cosets and Quotient Groups

As usual, definitions and examples, but we *might* want to break this down a little with additional examples to make sure it really sticks.

### 3.1 Lagrange's Theorem

This is so cool.

## 4 The Rubik's Cube Group

We'll introduce the notations for moves and how the moves are actually generators for the whole set. I think we might want to talk about group actions before this point but I'm not yet sure.

### 4.1 Coset Spaces

I don't know what these are yet.

### 4.2 Thistlethwaite's Algorithm

But this algorithm uses coset spaces, so we need to talk about those before we introduce it.