Supplementary Abstract Algebra Notes

Frank Thorne

March 14, 2024

Abstract

Notes for Math 546 (Algebraic Structures I), taught at USC in Spring 2024.

These are designed to supplement Nathan Carter's *Visual Group Theory* by going into a bit more detail on the formal aspect of the subject.

5 (January 19). Formal definition of groups.

Definition. A **group** is a set G with a binary operation $\cdot$ satisfying the following three axioms.

(1) There is an **identity** $e \in G$, with $e \cdot g = g \cdot e = g$ for every $g \in G$.

(2) Every $g \in G$ has an **inverse** $g^{-1} \in G$ satisfying $g \cdot g^{-1} = g^{-1} \cdot g = e$.

(3) The operation is **associative** in the sense that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$.

Formally, a **binary operation** is any function $G \times G \mapsto G$. Less formally, a binary operation is a 'multiplication rule' which takes as input two elements of G, and outputs a single element of G. By definition of 'binary operation', a group is always **closed** under the group operation: the product of two or more elements of G will itself be an element of G.

The binary operation $\cdot$ is often written with different notation. The notation $*$ is used in the book. Often, no notation is used at all: one writes gh for $g \cdot h$, in the same way that one writes $3x$ for 3 times x. Sometimes we write $+$ instead, when the group operation is more naturally interpreted as addition (see $\mathbb{Z}$ below for an example).

Comparison to Carter's informal definition. Two things are missing in comparison to the working definition in Carter's book, and the examples you have seen so far.

The first is any set being acted upon. Our first example was the Rubik's Cube group – a group with exactly 43,252,003,274,489,856,000 elements in it. As we emphasized in class, although we used the cube to define the group, the cube was itself not the group!

As another example, consider the group S_3. We defined this in class as the set of permutations of three cards, which we labeled 1, 2, and 3. These three cards are not part of the definition of the group – only the six group elements and the relations they satisfy. That said, the three cards definitely help us to understand what's going on!

Note that a 'group action' may also be given a formal definition, but we won't do this for now.

The second omission is any mention of **generators** for the group. For the Rubik's cube group, the group was naturally generated by F, B, L, R, U, D – 90 degree clockwise rotations of the front, back, left, right, top (up), and bottom (down) faces. For the group $V_4 = \{e, H, V, HV\}$, we chose the generators H (horizontal flip) and V (vertical flip).

These generators help us understand the group, and you need to choose a set of generators to draw a Cayley diagram. However, they are not part of the definition of the group itself.

Examples

We will now present some examples which contrast to those presented so far in Carter's book – and, in particular, which are usually thought of without any group action or generators.

The integers $\mathbb{Z}$. The set of integers $\mathbb{Z}$ forms a group, with addition as the group operation and 0 as the identity. Here we write $+$, 0, and $-n$ in place of $\cdot$, e, and n, so that we can write $2 + (-2) = 0$ instead of $2 \cdot (2^{-1}) = e$.

This is our first example of an infinite group. The inverse of an integer n is $-n$, and the associative law is familiar from arithmetic.

The group $\mathbb{Z}$ can be generated by the single element 1, and this produces the following Cayley diagram: (draw on board)

Alternatively, the group $\mathbb{Z}$ can be generated by the single element -1. (Draw) There are other possibilities too, for example the set $\{2, 3\}$. (Draw)

In-class discussion exercise. Which of the following subsets of the integers form groups? Why or why not?

(a) The **nonnegative integers** $0, 1, 2, 3, \cdots$

(b) The **even integers**.

(c) The **odd integers**.

(d) The set of all multiples of 17.

(e) The integers, only with multiplication as the group operation instead of addition. If they are not a group, can you find a subset of the integers that forms a group with this group operation?

The real numbers $\mathbb{R}$. This set also forms a group, again with addition as the group operation and 0 as the identity. This is a bigger group than $\mathbb{Z}$, which contains $\mathbb{Z}$ as a *subgroup*. (We will have much more to say about subgroups later!)

It is pretty well impossible to draw a Cayley diagram for this group, even if one is willing to use 'dot dot dot' as shorthand for 'and so on'. The set $\mathbb{R}$ is **uncountably infinite**, and there is *no* finite subset of $\mathbb{R}$ which generates the whole set. There is not even a countably infinite generating set.

Regrettably, Hagoromo does not sell boxes of chalk with uncountably infinitely many different colors, and so we cannot attempt to draw a Cayley diagram.

Other 'number' examples. The sets $\mathbb{Q}$ (rational numbers) and $\mathbb{C}$ (complex numbers) also form groups, again with the same examples. There are other subsets of $\mathbb{R}$ which also form groups; for example, the set

$$\{a + b\sqrt{2} \ : \ a, b \in \mathbb{Z}\}$$

is a group, and $\{1, \sqrt{2}\}$ is a generating set.

Matrices. From your previous course on linear algebra, you have seen **matrices**. For simplicity, I will focus on 2×2 matrices with real number entries. Recall the following facts from linear algebra:

- It is possible to **multiply** two matrices. (*Do an example.*) This operation is associative, and it is not commutative.
- 2×2 matrices represent linear transformations $\mathbb{R}^2 \mapsto \mathbb{R}^2$. (*Review this.*) If we do this, then matrix multiplication corresponds to composition of linear transformations.
- There is an **identity** matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. This matrix represents the identity linear transformation, and it satisfies $IM = MI$ for all 2×2 matrices M.

- A matrix may or may not be invertible, and there are lots of equivalent conditions for a matrix to be invertible. (The rows are linearly independent; the columns are linearly independent; the nullspace consists only of the zero vector; the determinant is nonzero; etc.) The inverse of an invertible matrix is invertible, and the product of two invertible matrices is invertible.

So can we make the set of matrices into a group? There is an associative binary operation (matrix multiplication), there is an identity I, and at least *some* matrices are invertible.

6 (January 22). Continued:

Since not *all* matrices are invertible, the set of 2×2 matrices does not form a group. However, if we restrict to the invertible matrices, notice that (1) this subset contains the identity; (2) it is closed under inverses and the binary operation. That means that the set of 2×2 invertible matrices *does* form a group. This group has a name:

Definition. The **general linear group** $\mathrm{GL}(2, \mathbb{R})$ is the set of 2×2 invertible matrices. It forms a group, with matrix multiplication as the group operation and I as the identity.

More generally, $\mathrm{GL}(n, \mathbb{R})$ is the group of $n \times n$ invertible matrices. There are also many other fascinating subgroups of $\mathrm{GL}(n, \mathbb{R})$ or $\mathrm{GL}(n, \mathbb{C})$: **special** linear groups, **orthogonal** groups, **symplectic** groups, **unitary** groups... when one considers these groups with their geometric structure, one has a **Lie group**. Lie groups are fascinating and beautiful and you may want to study them in some later course.

The integers mod m. Let m be a positive integer. Then, we can consider the **group of integers mod m**. Carter uses the notation $\mathbb{Z}_m$ for this group; it is 'more properly' denoted $\mathbb{Z}/m$ or $\mathbb{Z}/m\mathbb{Z}$, but we will follow Carter's notation in these notes.

There are two (equivalent) ways to define this group. Here is the more lowbrow of the two. The group elements of $\mathbb{Z}_m$ are the integers $0, 1, \ldots, m-1$, and the group operation is 'addition (mod m)' which means ordinary addition, but if the result is $\geq m$ then you subtract m.

As an example of this, in $\mathbb{Z}_5$, $2+2=4$, $0+3=3$, $2+3=0$, and $4+3=2$. In $\mathbb{Z}_4$ we have instead $2+2=0$, $0+3=3$, $2+3=1$, and $0+3=3$.

In this group, 0 is always the identity (for any m). What about inverses? For example, let's compute the inverse of 9 in $\mathbb{Z}_{13}$. We need to find some integer a, with $0 \leq a \leq 12$, and such that $a+9$ is either 0 or 13. We see that $a=4$ is the unique solution.

In general, in $\mathbb{Z}_m$, 0 is its own inverse, and the inverse of any other a is $13-a$.

These are **cyclic** groups – as can be seen by drawing a Cayley diagram with 1 as a generator. [Do a couple examples on the board.] The Cayley diagram makes a cycle, hence the name.

In general, a **cyclic group** is any group which can be generated by a single element. All the groups $\mathbb{Z}_m$ are examples, the group $\mathbb{Z}$ of integers is also an example, and 'up to isomorphism' these are the *only* cyclic groups.

An example of an isomorphism. We will formally define the notion of *isomorphism* later, but for now let us see an example.

Recall the group of rotations of a square, where we write R for rotation by 90 degrees. Then this group has four elements – e, R, R^2, and R^3 – with the relation $R^4 = e$. [Draw the Cayley diagram again.] You will notice that the Cayley diagram is the same as that for $\mathbb{Z}_4$, and that these groups have the same structure, with e corresponding to 0, and R^i corresponding to i for $i = 1, 2, 3$. (If you write $e = R^0$ then you can say that R^i corresponds to i for all i!) If you rotate 3 times and then 2 more times, then this is equivalent to rotating $3+2=5$ times, but it's also equivalent to rotating $3+2-4=1$ times, because the first four rotations just return you to the starting point.

So, these groups are 'the same', even though we described them differently.

First formal properties

Using the definition of a group, it is possible to prove various elementary formal properties. Here are two examples.

Proposition 1 (Cancellation laws) *Let a, b, c be elements of a group G.*

(i) Suppose that $ab = ac$. Then $b = c$.

(ii) Suppose that $ba = ca$. Then $b = c$.

Proof: We will prove only the first statement – the proof of the second is exactly similar.

Suppose that $ab = ac$. Then, there exists an element $a^{-1} \in G$ for which $a^{-1}a = e$. Hence, we have

$$\begin{aligned} ab &= ac && \text{(given)} \\ a^{-1}(ab) &= a^{-1}(ac) && \text{(multiply by } a^{-1} \text{ on both sides)} \\ (a^{-1}a)b &= (a^{-1}a)c && \text{(associative law)} \\ eb &= ec && \text{(property of inverses)} \\ b &= c. && \text{(property of identity element)} \end{aligned}$$

□

We said that there is *an* identity. Can there be a second?

Proposition 2 (Uniqueness of the identity) *In a group G, suppose an element f satisfies $f \cdot g = g \cdot f = g$ for every $g \in G$. Then $f = e$.*

Proof: By hypothesis, we have $f \cdot g = g$ for every g, and in particular $f \cdot e = e$. Since e is an identity, $f \cdot e = f$. Therefore, $f = e$. □

Here are two similar propositions, whose proofs we leave for the reader:

Proposition 3 (Uniqueness of inverses) *Let $g \in G$, and suppose that some $h \in G$ satisfies $g \cdot h = h \cdot g = e$. Then, $h = g^{-1}$.*

In fact, you can do a little bit better: if $g \cdot h = e$ **or** $h \cdot g = e$, then $h = g^{-1}$.

Proposition 4 (Inverse of a product) *Let $g, h \in G$. Then, $(gh)^{-1} = h^{-1}g^{-1}$.*

To prove it, just do it formally. But to understand why it's true, think in terms of actions. In the morning, you put on your socks and then you put on your shoes. If you want to undo these, you undo each step – in the opposite direction!

Similarly, if you want to undo a sequence of actions with a Rubik's cube, then you would undo each of them in the opposite order. [Demonstrate.]

At this point, we will return to Carter's approach, where in Chapter 5 he presents five families of groups that are nicely analyzed visually.

Exercises for HW 2

1. Prove Proposition 3.
2. Define
$$\mathrm{SO}(2, \mathbb{R}) := \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \ : \ \theta \in \mathbb{R} \right\},$$
the *special orthogonal group.*

(a) Prove that this is a group. For the associative law, you are encouraged to find a shortcut instead of doing a messy computation.

(b) Draw a picture of the linear transformation represented by a typical element of $\mathrm{SO}(2,\mathbb{R})$. Based on your picture, give a geometric description of $\mathrm{SO}(2,\mathbb{R})$ as a whole, and a geometric justification for why $\mathrm{SO}(2,\mathbb{R})$ is a group.

(c) (**Bonus**) Define a group which contains $\mathrm{SO}(2,\mathbb{R})$ and which is 'twice as large', and which is defined in analogy to the dihedral groups. (The instructions are deliberately ambiguous – the hard part is figuring out what this should mean!) Show that your group contains D_n for every integer $n \geq 1$.

11 (February 2). More on the Symmetric Group

Recall the definition of the *symmetric group* S_n from Carter's book and from class. Recall also our *cycle notation*; for example, in S_7, the element $(247)(53)$ is shorthand for the permutation

$$1 \mapsto 1,\ 2 \mapsto 4,\ 3 \mapsto 5,\ 4 \mapsto 7,\ 5 \mapsto 3,\ 6 \mapsto 6, 7 \mapsto 2.$$

The notations $(247)(35)$ and $(472)(35)$, among three others, all refer to the same permutation (and the same element of S_7).

Yet another notation is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 5 & 7 & 3 & 6 & 2 \end{pmatrix}.$$

We want to do some example computations. But first we have to deal with a nuisance that will pop up...

Notational interlude. Which function comes first?

At this point we run into an annoying technicality: if we want to do one permutation after another, then one must choose in which order to write them. This is easy, right? Not so fast – let us consider two examples.

- Think about the group D_4 – rotations of a square, generated by R (rotate 90 degrees) and H (flip horizontally). Suppose you write RH. What does this mean? Do R first, then H, clearly. This is how we explained things previously, and it makes the most sense in terms of the Cayley diagram. What could be more natural?

- Now think back to when you saw *function composition* in precalculus. Let $f(x) = x^2$ and $g(x) = x^3+1$? What is the composite function $f \circ g$? It looks like it should mean 'do f first, then g', but we compute

$$(f \circ g)(x) = f(g(x)) = f(x^3+1) = (x^3+1)^2 = x^6 + 2x^3 + 1.$$

  In other words, $f \circ g$ means do g first, then f. Although f and g aren't elements of a group, you can think of functions as 'acting on numbers', so the situation is analogous.

Why is this necessary? This notation would be all so much nicer if we wrote functions *after* their inputs. For example, $(x)\sin$ instead of $\sin(x)$. That way, if we wrote $((x)\sin)\cos)$, then we would apply the two trig functions in the order we saw them: take the sine of x first, then the cosine of the result. Alas, we are stuck with convention. Whenever you write functions on the left, this means that you apply them in reverse order. If these functions are elements of a group, then this is called a 'left group action'.

In these notes, we will apply the 'right group action' convention: writing fg will always mean 'do f first, then g'. This is consistent with Carter's book, and with the natural idea that actions should be written in the order that you do them. **But beware:**

1. The opposite is a more common convention in most treatments of group theory. For example, the Wikipedia page on the symmetric group adopts the opposite convention, as do books by e.g. Saracino and by Dummit and Foote.

2. The opposite is also used in linear algebra. Let $M, N \in \mathrm{GL}(n, \mathbb{R})$ – recall this means that M and N are invertible $n \times n$ matrices. Each of these matrices represent linear transformations $\mathbb{R}^n \mapsto \mathbb{R}^n$, which are special types of functions, and MN represents the linear transformation 'do N first, then M'.

3. With this convention, we have $(fg)(n) = g(f(n))$ – and the swap in order might come as a surprise.

12 (February 5). More on the Symmetric Group, Continued

Example. Let

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 5 & 7 & 3 & 6 & 2 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 1 & 3 & 5 & 7 & 4 \end{pmatrix}.$$

1. Write f and g using the other two notations: Carter's arrow notation, and cycle notation.

2. Compute fg, gf, and f^2.

3. Compute the **orders** of f and g: the smallest integers n and m for which $f^n = e$ and $g^m = e$.

4. Find elements of S_7 whose orders are: 1, 2, 3, 4, 5, 6, 7, 10, and 12. Can you find any others?

5. Find some pairs of elements of S_7 which commute with each other. When does this happen? Can you find a condition that would guarantee this? Can you find a different condition that would (separately) guarantee this?

Solutions.

1. We omit the arrow notation, but we have $f = (247)(35)$ and $g = (126743)$.

2. We have

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 5 & 4 & 1 & 7 & 6 \end{pmatrix}, \; gf = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 1 & 5 & 3 & 2 & 7 \end{pmatrix}, \; f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 3 & 2 & 5 & 6 & 4 \end{pmatrix}.$$

   In cycle notation, we have

$$fg = (1235)(67), \; gf = (1463)(26), \; f^2 = (274).$$

   Note that fg and gf look different from each other and from f and g – there are no obvious patterns here. The cycle structure from f^2 is somewhat more predictable, as the cycles (247) and (35) can be looked at repeatedly: $(247)^2 = (274)$, and $(35)^2 = e$.

   Also, our solution depends on our right action convention: fg means do f first, then g. If we adopted the left action convention, the answers for fg would be swapped. The answer for f^2 is the same using either convention, since f commutes with itself.

3. (In summary) Notice that disjoint cycles operate independently! For f, powers of the cycle (247) return to the identity every multiple of 3, and powers of (35) return every power of 2. So $f^k = e$ whenever e is a multiple of 6, and so the order of f is 6.

   Similarly the order of g is 6.

4. (In summary) We can use the 'least common multiple' rule as sketched in the previous step. So, for example, (12345)(67) has order 10. There are no others.

5. (In summary) There are at least two distinct conditions that guarantee that two elements will commute: (1) any element will always commute with a power of itself; and (2) two elements of S_n will commute if their cycle structures are disjoint.

The second rule is particularly nice. Suppose that one looks at the following element of S_7:

$$(146)(235)(147)$$

This is *not* a standard way of notating a single element of S_7; it is preferred to write each element so that the cycles are disjoint. However, we can interpret the above in terms of group multiplication: is it

- (146), followed by (235), followed by (147), or
- (146)(235), followed by (147), or
- (146), followed by (235)(147)?

The answer is *yes*, all of the above.

Here is a fundamental result.

Proposition 5 *Let g be any element of S_n. Then, $g^{n!} = e$, and in particular g has order at most $n!$.*

Proof: We can write g in terms of its cycle structure, and each cycle will have some order in $\{1, 2, 3, \ldots, n\}$. g^k will be the identity if k is a multiple of the lengths of each of the cycles. In particular, this is guaranteed if k is a multiple of each of $1, 2, \ldots, n$. $\square$

In fact, more is true. As we saw above, any element of S_7 has order at most 12, and dividing 420. But general rules like this are a bit hard to prove.

Also, as we will see later, we always have $g^{|G|} = e$ for any element g of any finite group G.

So *any* permutation in S_n, if repeated often enough, will return to the identity. Here is a dramatic example of an element of S_{52} of order 8:

`https://www.youtube.com/watch?v=rEoYwyHddLc`

Why does this work? (**Explain in much more detail in class**) Label the card positions $0, 1, 2, \ldots 51$. (We could label them 1 through 52, but by starting with 0 the pattern will be clearer.) We see that the Faro shuffle is the permutation

$$0 \mapsto 0,\ 1 \mapsto 2,\ 2 \mapsto 4, \ldots\ 25 \mapsto 50,$$

and

$$26 \mapsto 1,\ 27 \mapsto 3,\ 29 \mapsto 5, \ldots,\ 51 \mapsto 51.$$

This can be succinctly described by $x \mapsto 2x \pmod{51}$ for every x.

0 and 51 are fixed points of the shuffle: the top card will always be on top, and the bottom card will always be on bottom. As for 1, the cycle is $(1, 2, 4, 8, 16, 32, 13, 26)$. (We include commas here because the numbers run into double digits!) This cycle has length 8. The next cycle is $(3, 6, 12, 24, 48, 45, 39, 27)$, also of length 8, and we find that *all* cycles are of length 8. So the permutation has order 8.

Why do the permutations all have order 8? To explain this, we want to use the $x \mapsto 2x \pmod{51}$ formulation. Starting with any x, its cycle will be

$$(x, 2x, 4x, 8x, 16x, 32x, 64x, 128x),$$

where we take the least residue $\pmod{51}$ – i.e. where we divide by 51 and keep only the remainder. The next element would be $256x$, but notice that $256 = 5 \cdot 51 + 1$, so $256x$ reduces to $x \pmod{51}$ and the cycle repeats.

13. Matrix representations and the alternating group

Matrix representations of the symmetric group

It is also possible to represent elements of the symmetric group as matrices. For example, consider the matrix

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

and let $v_1 = (1, 0, 0)^T$, $v_2 = (0, 1, 0)^T$, and $v_3 = (0, 0, 1)^T$ be the standard basis elements of $\mathbb{R}^3$. Then, we have $Mv_1 = v_1$, $Mv_2 = v_3$, and $Mv_3 = v_2$. Therefore, we can think of M as representing the element

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

of S_3.

Definition. An $n \times n$-**permutation matrix** is any $n \times n$ matrix satisfying the following:

- There is exactly one 1 in every row.
- There is exactly one 1 in every column.
- All of the other entries are zero.

By construction, permutation matrices correspond exactly to elements of the symmetric group. This is a bijection of sets, and in fact you can check that much more is true:

- The identity permutation corresponds to the identity matrix.
- If a matrix M_g corresponds to the element $g \in S_n$, then its inverse $(M_g)^{-1}$ corresponds to g^{-1}.
- Matrix multiplication also corresponds to group multiplication in S_n! However, this correspondence is subject to our 'which action comes first' discussion: matrix multiplication is usually defined so that the *second* linear transformation is done first.

  Therefore, if M_g corresponds to g, and M_h corresponds to h, the matrix $M_h M_g$ corresponds to gh.

You can also check (if you remember your linear algebra!) that any such matrix has rank n, is invertible, and has determinant either 1 or -1.

Transpositions and the alternating group

Definition. A *transposition* in S_n is any permutation that swaps two elements and keeps all the others fixed. It is "obvious" that S_n is generated by transpositions. To convince yourself of this, imagine that you had a list of the numbers 1 through 10 and needed to sort them. Then, it would be possible to do this by only swapping two at a time. For example, if 1 is not in the first position, then swap it with whatever is. Then, if 2 is not in the second position, swap it, and so on.

A formal proof would spill a lot of ink; writing one out is left as an exercise for the reader, which the reader should probably choose to skip.

We can also see that the matrix corresponding to a transposition has determinant -1, since it is obtained from the identity by swapping two rows.

Definition. A permutation $g \in S_n$ is *even* if it can be written as a product of an even number of transpositions, and *odd* it it can be written as a product of odd transpositions. For example, in S_5, (123)

is even because we have

$$(123) = (21)(32) = (14)(12)(43)(42).$$

Clearly, any permutation is either even or odd. But why not both? Perhaps there is a permutation which can be written as a product of four transpositions one way, and five another way?

To see that this can't happen, we rely on the linear algebra that we have just described. If a permutation is even, then its determinant is -1 raised to an even power, so 1. If a permutation is odd, then its determinant is -1 raised to an odd power, so -1. Since the determinant cannot be both 1 and -1, a permutation cannot be both even and odd.

This is **not** a trivial theorem! In most group theory textbooks, it is given a rather involved proof. So how did we prove it so cheaply? The secret is that the existence of a determinant function, satisfying $\det(MM') = \det(M)\det(M')$, is *also* not a trivial theorem, and essentially the same work was done there, so we rely on *that*.

Definition. The **alternating group** consists of all of the even permutations in S_n.

Notice that this really is a group: the identity is even (it is the product of zero permutations); the inverse of an even permutation is an even permutation (do all the transpositions in the opposite order); the product of two even permutations is an even permutation (do an even number of transpositions, followed by another even number of transpositions).

Which cycle types are in the alternating group?

Proposition 6 *An n-cycle can be written as a product of $n-1$ transpositions.*

Proof: Without loss of generality assume that the n-cycle is $(12\ldots n)$; then, we have

$$(12\ldots n) = (12)(13)(14)\ldots(1n).$$

□

Therefore, if an element of S_n has cycles of length $\ell_1, \ldots, \ell_k$, this element can be written as a product of

$$\sum_{i=1}^{k} (\ell_i - 1)$$

transpositions. So, for example, in S_5, we see that A_5 contains the following elements:

- The identity (1 element);
- The 3-cycles (20 elements);
- The pairs of transpositions (15 elements);
- The 5-cycles (24 elements).

Note that

$$1 + 20 + 15 + 24 = 60.$$

The size of the alternating group

We have $|S_n| = n!$. It stands to reason that perhaps half of S_n should consist of even permutations, and half of odd. Indeed this is the case:

Proposition 7 *If $n \geq 2$, we have $|A_n| = n!/2$.*

Proof: Let g be any element of S_n not in A_n; for example, take $g = (12)$. Now we enumerate the elements of A_n:

$$A_n = \{h_1, \ldots, h_k\},$$

and consider the set

$$\{gh_1, \ldots, gh_k\}. \tag{1}$$

Then these are all distinct odd permutations, so there are at least as many odd permutations as there are even.

Moreover, I claim that every odd permutation appears somewhere in the list (1). For, if γ is an odd permutation, then $g^{-1}\gamma$ is even and hence $g^{-1}\gamma = h_i$ for some i, and gh_i indeed appears on the list (1). □

The principle behind Proposition 7 will *vastly* generalize: we will prove by means of *cosets* that if H is a *subgroup* of G, we have $|H| \mid |G|$.

Exercises

1. Let
$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 3 & 2 & 1 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 5 & 3 & 1 & 4 \end{pmatrix}$$
be two elements of S_6.
   (a) Write f and g using the other two notations: Carter's arrow notation, and cycle notation.
   (b) Compute fg, gf, and f^2.
   (c) Compute the orders of f, g, fg, gf, and f^2.
   (d) Determine whether each of the elements in f, g, fg, gf, and f^2 is in A_6 or not.
   (e) Compute all possible orders of elements in S_6, and give examples of each.
   (f) Compute all possible orders of elements in A_6, and give examples of each.
2. Describe all possible cycle types of elements in A_6, and compute how many elements A_6 has of each type.

   Your answers should sum to 360!

25. Homomorphisms

Definition. Let G and H be groups. A homomorphism from G to H is any function ϕ with $\phi(gg') = \phi(g)\phi(g')$ for all g and g' in G.

As boring examples, the identity map from any group G to itself is always a homomorphism. Also, if G and H are any groups, the map sending any element in G to $e \in H$ is a homomorphism.

Example 8 *Let $G = \mathrm{GL}(n, \mathbb{R})$, for some fixed positive integer n. Then, the* **determinant** *is a homomorphism from G to $R^\times$, because*

$$\det(gg') = \det(g)\det(g')$$

for all matrices g and g' with determinant $\neq 0$.

(In fact, this equation is also true when the matrices have determinant 0 – but that's outside the scope of our discussion now.)

Example 9 *Let* $\mathbb{C}$ *be the* **complex numbers**

$$\mathbb{C} := \{a + bi \ : \ i^2 = -1\}.$$

This forms a group, with addition as the group law. Define a map $\phi : \mathbb{C} \mapsto \mathbb{C}$ *by*

$$\phi(a + bi) = a - bi.$$

Then ϕ *is a homomorphism (called* **complex conjugation***).*

To check this, let $a + bi$ and $c + di$ be arbitrary complex numbers. Then,

$$\phi((a + bi) + (c + di)) = \phi((a + c) + (b + d)i) = (a + c) - (b + d)i,$$

and

$$\phi(a + bi) + \phi(c + di) = (a - bi) + (c - di) = (a + c) - (b + d)i,$$

and these are the same.

In fact, this ϕ has some interesting additional properties. For one, since ϕ is a bijection, it is invertible, and ϕ^{-1} is a homomorphism as well. (In fact, $\phi^{-1} = \phi$, but that's not what makes this interesting.) This makes ϕ into an **automorphism** of the group $\mathbb{C}$.

Moreover, we also have

$$\phi((a + bi)(c + di)) = \phi(a + bi)\phi(c + di),$$

as you can readily check. This is outside the scope of our current discussion, as groups only have one operation. But the fact that $\mathbb{C}$ has both addition and multiplication rules (with certain properties...) makes it into a **ring** and **field**, and this same ϕ is also a ring automorphism and a field automorphism. If you take further courses in abstract algebra, you are likely to see much more about rings and fields.

Example 10 *This example will explain how linear transformations (from linear algebra) are examples of homomorphisms.*

Let V and W be real vector spaces. (Less generally, imagine $V = W = \mathbb{R}^n$ if that makes things easier.)

Recall that vector spaces have **addition** and **scalar multiplication**, and are required to satisfy a lot of axioms. If we ignore the axioms that involve scalar multiplication, then a vector space V is required to satisfy the following:

- $x + y = y + x$ for all $x, y \in V$.
- $(x + y) + z = x + (y + z)$ for all $x, y, z \in V$.
- There exists $0 \in V$ such that $0 + x = x$ for all $x \in V$.
- For every $x \in V$, there exists $-x \in V$ with $x + (-x) = (-x) + x = 0$.

These are exactly the axioms of an abelian group! So you can think of vector spaces as 'abelian groups with extra structure'.

Now, a linear transformation is any function ϕ from V to W which satisfies the following two axioms:

- $\phi(x + y) = \phi(x) + \phi(y)$ for all $x, y \in V$.
- $\phi(\lambda x) = \lambda\phi(x)$ for all $x \in V$ and $\lambda \in \mathbb{R}$.

The first axiom says that a linear transformation must necessarily be a homomorphism of abelian groups! Indeed, a linear transformation is exactly the same thing as a homomorphism of vector spaces.

Example 11 *Let $G = D_4$, with presentation*

$$D_4 = \langle r, f \ : \ r^4 = f^2 = e, rf = fr^{-1} \rangle. \tag{2}$$

In this example we will construct several homomorphisms from D_4 to $\mathrm{GL}_2(\mathbb{R})$.

In other words, for each element $g \in D_4$ we will associate a 2×2 matrix $\phi(g)$, so that the corresponding matrices multiply in the same way.

First example. We define ϕ by

$$\phi(r) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \phi(f) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Note that we only said what ϕ did to the generators. We then **define** ϕ on all of D_4 so that it's a homomorphism, i.e. $\phi(rf) = \phi(r)\phi(f)$ and so on.

It's not a homomorphism just because we say it is – but when given a presentation of the form (2), it's enough to check that all the relations are satisfied. In other words, we need to check that

$$\phi(r)^4 = \phi(f)^2 = I, \ \phi(r)\phi(f) = \phi(f)\phi(r)^{-1}.$$

This is just an exercise in matrix multiplication. *Do at board.*

To really 'understand' this example, it is helpful to draw pictures to visualize what $\phi(r)$ and $\phi(f)$ 'do' to the plane. Doing this (do at board!), we see that r is rotation counterclockwise by 90 degrees, and f is flipping across the x-axis. So, if we think about D_4 as the rigid motions of our square, then this really does match up!

Variations. Suppose, that instead of the above, we had defined

$$\phi(r) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

which is clockwise rotation by 90 degrees. Then, this together with the above $\phi(f)$, also defines a homomorphism from D_4 to $\mathrm{GL}(2, \mathbb{R})$ – and not the same one! Don't take my word for it – do the calculations and check for yourself!

Similarly, we could have defined $\phi(f)$ to be a flip across the y-axis, instead of a flip across the x-axis. This, too, would have worked.

Second example. Define ψ by

$$\psi(r) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \psi(f) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then we can again check that all the relations are satisfied, so ψ is a homomorphism.

This homomorphism is quite different, because we have $\psi(r^2) = I$. Moreover, the image of ψ is abelian (isomorphic to V_4), even though G is not abelian.

Definition. The **kernel** of a homomorphism $\phi : G \mapsto H$ is the set of elements $g \in G$ for which $\phi(g) = e$. (That is, for which $\phi(g) = e_H$.)

In other words, it is the exact analogue of the **nullspace** of a linear transformation between two vector spaces. In your course in linear algebra, you proved a lot about nullspaces, and the kernel will enjoy some analogous structure.

Third example. Define α by

$$\alpha(r) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \alpha(f) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

In other words, rotation now does **nothing**, but the flip remains intact. This is again a homomorphism; its image consists of two matrices, and its kernel is $\langle r \rangle \simeq C_4$.

But suppose you attempted to define β by

$$\beta(r) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \beta(f) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

In other words, rotation is as normal, but the flip now does nothing. This is not a homomorphism! In particular, we don't have

$$\beta(r)\beta(f) = \beta(f)\beta(r)^{-1}.$$

It is easy to see why. Because $\beta(f) = I$, the above equation reduces to $\beta(r) = \beta(r)^{)}-1$ – and so whatever $\beta(r)$ is, it must be its own inverse. That leaves only two possibilities: I and $-I$.

In particular, we can see that **there is no homomorphism from D_4 to $\mathrm{GL}(2,\mathbb{R})$ whose kernel is exactly $\{1, f\}$.** There is a good reason for this! – and we will see why.

Example 12 (Do on Day 26!) *Let S_3 be the set of permutations of $\{1,2,3\}$, and let S_4 be the set of permutations of $\{1,2,3,4\}$. Then, we may regard S_3 as a subgroup of S_4, by identifying S_3 with the set of permutations in S_4 which fix 4.*

More properly, we have a **homomorphism** *from S_3 to S_4 by this identification, sending each $g \in S_3$ to the corresponding permutation (fixing 4) in S_4. This type of homomorphism is called an* **embedding**, *as it shows how one group may be regarded as a subgroup of another.*

Example 13 (Day 26) *Let $G = S_3$ be the set of permutations of $\{1,2,3\}$, and let H be the set of permutations of $\{A,B,C\}$. Then, there is a homomorphism ϕ from G to H, obtained by identifying 1 with A, 2 with B, and 3 with C – for example, ϕ maps (132) to (ACB).*

This particular ϕ is one-to-one and onto, i.e., it is a **bijection**. *A bijective homomorphism is called an* **isomorphism**; *its inverse will also be a homomorphism and isomorphism.*

Example 14 (Day 26) *Let G be the following subgroup of S_4, which you saw on the exam:*

$$G = \{e, (12)(34), (13)(24), (14)(23)\}.$$

Then, on the exam you determined that G has the same structure as V_4. Although you can say that G 'is' V_4, it is more precise to say that G is isomorphic to V_4.

For example, if we write

$$V_4 = \langle a, b \ : \ a^2 = b^2 = e, ab = ba \rangle,$$

then one isomorphism ϕ from G to V_4 is: $\phi(e) = e$, $\phi((12)(34)) = a$, $\phi((13)(24)) = b$, and $\phi((14)(23)) = ab$.

This is not the only isomorphism. Indeed, you can send any of the nonidentity elements of G to any of the nonidentity elements of V_4 in any combination. (Caution! This is particular to V_4.)

26. Homomorphism Properties

Proposition 15 *Let $\phi : G \mapsto H$ be a homomorphism. Then $\phi(e) = e$.*

More specifically, this means that $\phi(e_G) = e_H$, where e_G and e_H are the identity elements of G and H respectively.

Proof: We have

$$\phi(e_G) = \phi(e_G \cdot e_G) = \phi(e_G) \cdot \phi(e_G).$$

(Here all of these are elements of H.) Cancelling $\phi(e_G)$ from each side of the equation, we obtain

$$\phi(e_H) = \phi(e_G).$$

□

This is a direct analogue of the theorem from linear algebra that a linear transformation must map 0 to 0.

Similarly, we have:

Proposition 16 *Let $\phi : G \mapsto H$ be a homomorphism. Then $\phi(g^{-1}) = \phi(g)^{-1}$ for every $g \in G$.*

Proof: We have

$$e = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}),$$

proving the claim. □

Proposition 17 *Let $\phi : G \mapsto H$ be a homomorphism. Then,* $\mathrm{Ker}(\phi)$ *is a subgroup of G.*

Proof: It is clearly a subset of G, and satisfies the associative law since G does. It contains the identity and is closed under inverses by the previous two propositions, so we must show that it is closed under multiplication. This is the same idea. Namely, if $g, g' \in \mathrm{Ker}(\phi)$, then

$$\phi(gg') = \phi(g)\phi(g') = e \cdot e = e,$$

so $gg' \in \mathrm{Ker}(\phi)$. □

It is similarly possible to check that $\Im(\phi)$ is a subgroup of H, and we leave the proof to the reader.

This all *completely analogous* to the following theorem from linear algebra: let $\phi : V \mapsto W$ be a linear transformation of vector spaces; then, the nullspace (kernel) of ϕ is a subspace of V, and the image of ϕ is a subspace of W.

Proposition 18 *Let $\phi : G \mapsto H$ be a homomorphism, and let h be any element in the image of ϕ. Then,*

$$\phi^{-1}(h) = \mathrm{Ker}(\phi) \cdot g = g \cdot \mathrm{Ker}(\phi),$$

for any g for which $\phi(g) = h$.

So, in other words, the inverse images of elements in H are all left cosets – and right cosets – of $\mathrm{Ker}(\phi)$.

Proof: We will prove that $\phi^{-1}(h) = \mathrm{Ker}(\phi) \cdot g$; the proof of the second assertion is exactly similar.

First of all, given an element of $\mathrm{Ker}(\phi) \cdot g$, we may write it as $g'g$ where $g' \in \mathrm{Ker}(\phi)$. Then we have

$$\phi(g'g) = \phi(g')\phi(g) = e \cdot h = h,$$

so $g'g \in \phi^{-1}(h)$, as desired.

Conversely, suppose that $g' \in \phi^{-1}(h)$. Then we have that

$$\phi(g'g^{-1}) = \phi(g')\phi(g)^{-1} = hh^{-1} = e,$$

so that $g'g^{-1} \in \mathrm{Ker}(\phi)$, and hence $g' \in \mathrm{Ker}(\phi) \cdot g$. □

Since, for every $g \in G$, we can apply the proposition to $\phi(g)$, we immediately obtain the following as corollary:

Theorem 19 *Let $\phi : G \mapsto H$ be a homomorphism. Then, its kernel is a normal subgroup of G.*