MAT301 - GROUPS & SYMMETRIES

PATRICK J ROBINSON

Contents

0. Introduction, $\mathrm{GL}(n, \mathbb{R})$, Dihedral Groups

Groups are one of the most fundamental, and ubiquitous, objects in mathematics. They are at the heart of the idea of symmetry, as we will see explicitly through examples such as the dihedral and symmetric groups. Groups exist in many categories in mathematics, and are used to describe physical properties and systems in the natural sciences.
Groups are everywhere, and describe many things.

0.1. $\mathbf{GL}(n, \mathbb{R})$.

One of the examples of a group we are (unknowingly) already familiar with, having worked with it a lot in our previous linear algebra days, is the set of invertible $n \times n$ matrices, $\mathrm{GL}(n, \mathbb{R})$ (which stands for "general linear" group). In set-builder notation:

$$\mathrm{GL}(n, \mathbb{R}) = \{A \in \mathrm{Mat}_{n\times n}(\mathbb{R}) \mid \det(A) \neq 0\}$$

(1) If we have two invertible matrices, A and B, we know that the product AB must also be invertible. This is because $\det(AB) = \det A \det B$, and so if $\det A \neq 0$, $\det B \neq 0$, then $\det A \det B$ cannot be 0. This means that if $A, B \in \mathrm{GL}(n, \mathbb{R})$, then $AB \in \mathrm{GL}(n, \mathbb{R})$; we say, then, that $\mathrm{GL}(n, \mathbb{R})$ is "closed under matrix multiplication", since multiplying two elements of this specific set together always gives us something inside the set.

(2) Many of the proofs we did in linear algebra involved us taking advantage of being able to move the brackets of matrix multiplication around: we learned and showed that matrix multiplication is *associative*. This means that for all matrices A, B, C that we can multiply together in the appropriate fashion, we have that $(AB)C = A(BC)$. Since we can multiply any three elements of $\mathrm{GL}(n, \mathbb{R})$ together, this means that the multiplication in $\mathrm{GL}(n, \mathbb{R})$ must be associative as well.

(3) We also learnt of the *identity matrix*; an invertible matrix (usually denoted I_n, where n denotes how many rows) which does not change any matrix it multiplies. i.e.: for any $A \in \mathrm{GL}(n, \mathbb{R})$, $AI_n = I_nA = A$. We know that this is the diagonal $n \times n$ matrix with 1s along the diagonal

(4) Relatedly, we know that for any $A \in \mathrm{GL}(n, \mathbb{R})$, there exists another matrix in $\mathrm{GL}(n, \mathbb{R})$, denoted A^{-1}, which obeys the rule that $A^{-1}A = AA^{-1} = I_n$. This is called the *inverse of* A. Computing the inverse can be a very tedious affair, but luckily this is why computers were invented. As an easy example, for $n = 2$, we remember the formula that if

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ then } A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}. \tag{1}$$

We also remember that the operation of matrix multiplication is not *commutative*: for any $A, B \in \mathrm{GL}(n, \mathbb{R})$, AB does not necessarily (or generally) equal BA. For example, if $A = \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix}$, and $B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, then $AB = \begin{pmatrix} 5 & 2 \\ 1 & 0 \end{pmatrix}$, but $BA = \begin{pmatrix} 2 & 4 \\ 2 & 3 \end{pmatrix}$
The properties (1) – (4) above encode the things we will want our general notion of a "group" to have, though we will put off formally defining it until a little later (but it will look nearly identical to these already-listed properties). First we we will touch on another important example.

0.2. The Dihedral Group, D_3.

The dihedral groups help us to encode *symmetries* of regular shapes. The idea is, given a regular polygon in the plane (such as a triangle or a square) how can we move it around - without stretching or warping it - so that when we're done, it looks the same as when we started? Gallian goes through the example of the square, so to not be repetitive, we will go through the slightly easier example of the triangle. The first thing we should do to keep track of

the transformations we are going to apply to our triangle is to name the vertices: a, b, c.
Some of the first ideas for symmetries that come to mind are the ones obtained through rotating the shape (counter-clockwise), and reflecting the triangle through a specific line. We can name and summarise these as follows:

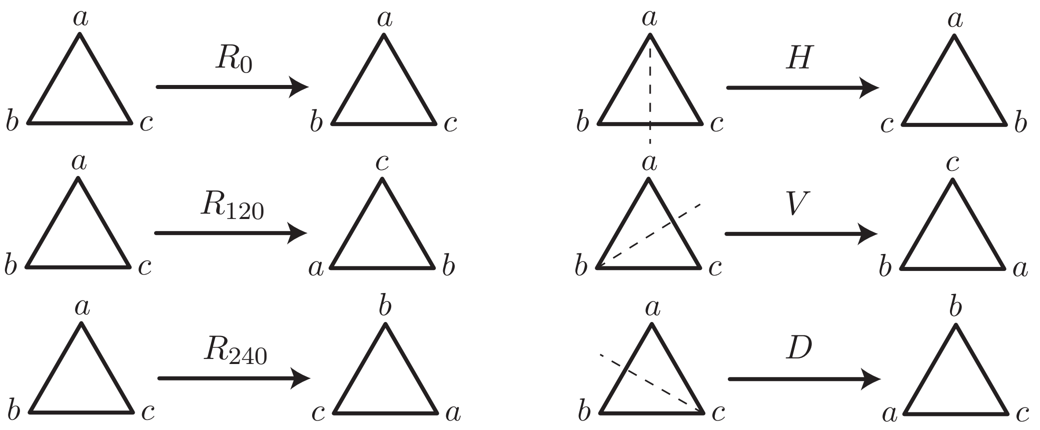

FIGURE 1. Rotations and Reflexions of the Triangle

Now we claim that these are the *only* symmetries of the triangle. There are 6 distinct symmetries listed in the above figure. Any symmetry of the triangle can send vertex a to any of the others, giving us 3 possibilities. Once we have chosen where a will go, we then have to choose b and c; we can either put them according to their original orientation with respect to a, or we can reflect them through the axis intersecting a, giving us two additional choices. Thus, in total, there are 6 symmetries of the triangle, meaning the symmetries in Figure 1 are the only symmetries of the triangle.
We notice too that we can compose two of the symmetries together by doing one, and then applying the second to the result of the first. For example, if we rotate by 180 degrees, and then we apply the reflexion described by V, this gives us the same result as just applying D. In composition notation, $V \circ R_{120} = D$. We will usually omit the $\circ$, and just write $VR_{120} = D$. We can put all of the possible compositions into a table, often called a *Cayley Table*, as follows:

	R_0	R_{120}	R_{240}	H	V	D
R_0	R_0	R_{120}	R_{240}	H	V	D
R_{120}	R_{120}	R_{240}	R_0	D	H	V
R_{240}	R_{240}	R_0	R_{120}	V	D	H
H	H	V	D	R_0	R_{120}	R_{240}
V	V	D	H	R_{240}	R_0	R_{120}
D	D	H	V	R_{120}	R_{240}	R_0

The way this table is read is the (element of the column) acts first, followed by the (element of the row). So for example, H acted first, followed by R_{120} gives D. i.e.: $R_{120}H = D$. We can easily see that composing R_0 with any element, first or second, will not change that element; in other words, for any A in the above table, we have $R_0A = AR_0 = A$. Also, we notice that for any A above, there

is a B such that $AB = BA = R_0$; no matter which symmetry we apply, there is always another symmetry which "undoes" the change we made, giving us the original set-up of the triangle. For the rotations, it's easy: for any rotation A, the B is going to be the rotation such that the angles add up to 360^o; so for $A = R_{120}$, the $B = R_{240}$. For the reflexions, we see $A = B$: $HH = R_0$, $VV = R_0$, and $DD = R_0$. We also note that, like in $\mathrm{GL}(n, \mathbb{R})$, the order in which we 'multiply' matters: $HR_{120} = V$, but $R_{120}H = D$, which are not the same. So the symmetries of the triangle are not commutative. Based on our $\mathrm{GL}(n, \mathbb{R})$ experience, we will most likely want the symmetries to be associative: $A(BC) = (AB)C$. We could try to check this for every possible set of three elements, but that would be incredibly tedious. Instead, we make note of what Gallian says, and see that since the multiplication here is just composition of functions, and we know that function composition is associative, this means we don't have to check anything. The set of symmetries of the triangle is called the dihedral group on three vertices, D_3. Indeed we will look soon at the symmetry of any n-sided regular polygon; this set is called the *Dihedral group of order 2n*, denoted D_n.
Important Note: There are two conventions for naming the dihedral groups. If you see D_n, the n could either refer to the number of vertices, or the total number of symmetries. We are following the first option, as does Gallian. So for the symmetries of the triangle, we called it D_3 because there are 3 vertices. In the other convention, we would have called the symmetries of the triangle D_6, since there are 6 symmetries. Trying to figure out which convention is being used can be annoying, so be forewarned if you use other resources, since they may use another convention. Remember for our course: D_n is the symmetries of a regular polygon with n vertices (for which there will be $2n$ symmetries).

1. Groups

1.1. **Definition and Examples.**

Having had inspiration from the two examples in the previous section, we are in a position to put down a concrete definition of a group. One of the things we noticed in both of the examples was that when we 'multiplied' any two elements of the sets we were looking at (matrices in $\mathrm{GL}(n, \mathbb{R})$, symmetries in D_3), we always got another element of the set. The multiplication never took us 'outside' the set; in mathematical terms, the operations are *closed*. We can define this as follows:

Definition 1.1. Let S be a set. A *Binary Operation* on S is a map that takes a pair of elements of S, and assigns to them another element of S. More precisely, it's a map $S \times S \to S$, taking a pair (a, b) to some other element c, for $a, b, c \in S$.

So in addition to the examples from the previous section, we also have a number of very familiar examples:

- The integers $\mathbb{Z}$, under addition
- The real numbers $\mathbb{R}$, under addition, or under multiplication
- The positive integers $\mathbb{Z}^+$ under addition

A non-example is the rationals $\mathbb{Q}$ under division: the map sending $(a, b) \mapsto a/b$ is not defined for all pairs $(a, b) \in \mathbb{Q} \times \mathbb{Q}$, namely for any $(a, 0)$. Hence, division is not a binary operation on $\mathbb{Q}$. (There is a way we can adjust this to make it a binary operation: restrict to only $\mathbb{Q}^+$, the positive rational numbers)

Definition 1.2. Let G be a nonempty set, with a binary operation (usually called *multiplication*) $G \times G \to G$ which takes $(a, b) \mapsto ab \in G$. We call G a **group** under this operation as long as all three of the follow properties are satisfied:

(1) *Associativity.* For all $g, h, k \in G$, we have $(gh)k = g(hk)$.

(2) *Identity.* There exists an element $e \in G$ such that for all $g \in G$, $ge = eg = g$.
(3) *Inverses.* For all $g \in G$, there exists an $h \in G$ such that $gh = hg = e$. This h is called the *inverse* of g, and is usually denoted by g^{-1}

Strictly from the definition, we can see that for any $g \in G$, $(g^{-1})^{-1} = g$. It is very important when given a potential group to make sure that the set is closed under the operation. As pointed out in example 5 of Gallian chapter 2, the set of irrational numbers under multiplication satisfies properties (1)-(3) in the above definition, but it isn't a group because it is not closed under multiplication: as a counter example, $\sqrt{2} \cdot \sqrt{2} = 2$, which isn't irrational.
Given a group G, if it's true that $gh = hg$ for *every* $g, h \in G$, then we say that the group is *Abelian*. If there is some pair $g, h \in G$ for which $gh \neq hg$, then G is *non-Abelian*. As a note, a common mistake is to think that if G is non-Abelian that this means that $gh \neq hg$ for all $g, h \in G$. This is not true: all you need is a single pair $g, h \in G$ for which $gh \neq hg$ to mean that G is non-Abelian. For example, the dihedral group D_3 we looked at in the previous section, we saw that $HR_{120} \neq R_{120}H$, which means that D_3 is non-Abelian. It does, however, have commuting elements; for example, $R_{120}R_{240} = R_{240}R_{120}$.
Examples

(1) The integers $\mathbb{Z}$ under addition. We already know addition is associative, and any two integers summed together gives another integer. In this case, the identity is 0, and for any $x \in \mathbb{Z}$, the inverse is $-x$. This group is Abelian.
(2) The real numbers $\mathbb{R}$ under addition. We know the sum of any two real numbers is also a real number; we still have $e = 0$ and $x^{-1} = -x$, and since addition commutes, this group is Abelian.
(3) The nonzero real numbers $\mathbb{R}^*$ under multiplication. Again, we know that multiplication is associative. Here, the identity is 1, and for any $x \in \mathbb{R}^*$, we have $x^{-1} = 1/x \in \mathbb{R}^*$. $\mathbb{R}^*$ is closed under multiplication because the product of two real numbers is real, and the only element in $\mathbb{R}$ not in $\mathbb{R}^*$ is zero, but if $xy = 0$, then either $x = 0$, or $y = 0$. Hence, the product of any two elements of $\mathbb{R}^*$ can never be zero, and so $(\mathbb{R}^*, \times)$ is closed. We also know that multiplication is commutative, so the group is Abelian.
(4) Any vector space V under vector addition. We know from linear algebra that associativity of vector addition is one of the axioms of a vector space. The zero vector $\overline{0}$ is the identity, and for any vector $v \in V$, the inverse is $-v$, and the group is Abelian. (In fact, a vector space has more structure than just this; it's also a *module*, but for our purposes we'll just view it as a group).
(5) $\mathrm{GL}(n, \mathbb{R})$ under matrix multiplication. We verified the properties back in section 1, and also saw that it is non-Abelian.
(6) The set of all $n \times m$ matrices with real entries $\mathrm{Mat}_{n\times m}(\mathbb{R})$ is a group under addition. Matrix addition is associative, the zero matrix is the identity, and for any $A \in \mathrm{Mat}_{n\times m}$, the additive inverse is $-A$. This is an abelian group. We will see later that the structure of $\mathrm{Mat}_{n\times m}(\mathbb{R})$ is the same ("isomorphic") to the vector space structure of $\mathbb{R}^{nm}$; i.e.: $\mathrm{Mat}_{n\times m}(\mathbb{R})$ is a real vector space of dimension nm
(7) The dihedral group D_3 under function composition. In fact, all dihedral groups D_n are (as you may have guessed by the name) groups under composition, and all are non-Abelian.
(8) Arithmetic modulo $n \in N$. The set $\{0, 1, 2, \ldots, n-1\}$, under addition modulo n is denoted $\mathbb{Z}/n\mathbb{Z}$ or just $\mathbb{Z}_n$. These form a class of very important examples to group theory
(9) The set $\mathbb{Z}_n \setminus \{0\}$ is a group under *multiplication* modulo n if and only if n is a prime number.
(10) Let S be any set, and let $G := \{\, f : S \to S \,|\, f \,\text{is a bijection}\,\}$. Then G is a group under function composition. To see this, consider $f_1, f_2 \in G$; we want to know if $f_1 \circ f_2$ is also in G, namely, if it is a bijection from S to itself. It clearly is a map from $S \to S$, sending $x \in S$ to

$f_1(f_2(x))$. Is it also a bijection? Well, to check 1-1, we want to know if $f_1(f_2(x)) = f_1(f_2(y))$, does this mean $x = y$? We know that both f_1, f_2 are $1-1$, so

$$\begin{aligned} f_1(f_2(x)) = f_1(f_2(y)) &\Rightarrow f_2(x) = f_2(y) \\ &\Rightarrow x = y \end{aligned}$$

Thus, $f_1 \circ f_2$ is $1-1$. Is it onto? For every $x \in S$, does there exist a $y \in S$ such that $f_1(f_2(y)) = x$? Well, f_1, f_2 are $1-1$, there exists an inverse function f_i^{-1} : $\text{range}(f_i) \to \text{domain}(f_i)$, for $i = 1, 2$ (such that $f_i \circ f_i^{-1} = f_0$, the function defined as $f_0(s) = s$ for all $s \in S$). Since f_1, f_2 are bijections, their domain and range are both all of S. Thus, for any $x \in S$, the element $f_2^{-1}(f_1^{-1}(x))$ is in S, and is mapped to x by $f_1 \circ f_2$. So $f_1 \circ f_2$ is onto as well as $1-1$, meaning it is a bijection, and so is in G.

Function composition is associative, so we don't have to check that. We also have mentioned that there is an identity function f_0 defined as $f_0(s) = s$ for all $s \in S$. Is this the identity of the group? i.e.: for any $f \in G$, is it true that $f \circ f_0 = f_0 \circ f = f$? Well, let $x \in S$, then:

$$f(f_0(x)) = f(x); \qquad f_0(f(x)) = f(x)$$

so yes, f_0 acts as an identity of G. Lastly, we want to check inverses, but we already checked that by using the inverse function theorem (and can now tie those inverses to f_0). Thus G is a group under function composition. It is not abelian (try to come up with a counterexample).

This is an important example of a group; groups we have yet to see (permutation groups), and some we have already seen ($\text{GL}(n, \mathbb{R})$) fit into this broad category.

(11) Consider $G = \{0\}$ under addition (or equivalently, $G = \{1\}$ under multiplication). This is an abelian group, called the *trivial group*. It is straightforward to check the group axioms.

There are many more examples to be found in Gallian chapter 2. Let's quickly talk about some non-Examples:

- The integers $\mathbb{Z}$ under subtraction are not a group, since subtraction is not associative. For example, $1-(2-3) = 2$, and $(1-2)-3 = -4$.
- The positive integers $\mathbb{Z}^+$ under addition. This cannot be a group because there is no identity element. If we look at the non-negative integers $\mathbb{Z}^+ \cup \{0\}$, this is still not a group: even though it has an identity, no element other than 0 has an inverse.
- The positive integers $\mathbb{Z}^+$ under multiplication is not a group because no element other than 1 has an inverse. There is no positive integer x such that $3x = 1$.
- The real numbers $\mathbb{R}$ under multiplication. The number $0 \in \mathbb{R}$ does not have a well-defined multiplicative inverse, so $(\mathbb{R}, \times)$ cannot be a group.
- The set of all $n \times n$ matrices with real entries $\text{Mat}_{n\times n}(\mathbb{R})$ is not a group under multiplication, since any determinant 0 matrix will not have an inverse.

1.2. **Basic Properties.** Now that we have a concrete definition of what a group is, we want to figure out what properties a group will have, regardless of what example we pick. We have to prove the things we conjecture from the definitions alone; we can use our intuition from the examples we've seen to point us in the right direction, but we cannot use a long list of examples of groups to prove anything about *all* groups. Examples are not proofs.

First, we will prove what is called the *Cancellation Law*. We know that for real numbers, $2x = 2y$ means that $x = y$; i.e.: we can 'cancel' the 2. Now we want to know, for any g, h, k in a group G, if it's true that $gh = gk$ means that $h = k$. In fact, this is true, and is our first theorem.

Theorem 1.1. Cancellation Let G be any group, and let $g, h, k \in G$ such that $gh = gk$. Then $h = k$.

Proof. If $gh = gk$, let us multiply on the left by g^{-1}. Then we get $g^{-1}(gh) = g^{-1}(gk)$. Now we use associativity to shift the brackets, and we get $(g^{-1}g)h = (g^{-1}g)k$, which means $eh = ek$, giving $h = k$ □

We know in all of the groups we've looked at that there has been only one identity. Also, for any element, there is only one inverse. Now we conjecture that this is true for all groups, and prove that:

Theorem 1.2. Uniqueness of Identity Let G be any group. There is only one identity element of G.

Proof. Let us suppose that there are two identities, e_1, e_2 in G. This means that for all $g \in G$, we have

(1) $ge_1 = e_1g = g$
(2) $e_2g = ge_2 = g$

By choosing $g = e_2$ in (1) we get $e_1e_2 = e_2$, and by choosing $g = e_1$ in (2), then we see that $e_1e_2 = e_1$. Thus, we have that $e_1 = e_2$. □

We've also seen in the previous groups that there's been only one inverse for a given element: in $\mathbb{R}$, the inverse of x is $-x$; in $\mathrm{GL}(n, \mathbb{R})$, we know the algorithm for computing the inverse of A, and it only gives us a single matrix. One might hope that for any group it's true that inverses are unique, since it would make our lives a lot easier. Luckily, the cancellation law helps us prove this:

Theorem 1.3. Uniqueness of Inverses Let G be a group. For any element $g \in G$, there exists a unique inverse g^{-1} for g.

Proof. Suppose that for $g \in G$, there exists two inverses, h, k such that

(1) $gh = hg = e$
(2) $gk = kg = e$

Since the expressions in (1) and (2) above are both equal to e, then we can equate them. We get that $gh = gk$, but by the cancellation law, this means that $h = k$. Thus, for any $g \in G$, the inverse of g is unique. □

Since Theorems 2.2 and 2.3 follow directly from 2.1, we could have called them Corollaries. Since they are important results, however, we choose to call them Theorems anyway. The next fact, however, we will call a Corollary to Theorem 2.3:

Corollary 1.1. Let G be a group. For any $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$.

Proof. For $g, h \in G$, consider (gh). If we multiply by $h^{-1}g^{-1}$, we see:

$$\begin{aligned}(gh)(h^{-1}g^{-1}) &= g(hh^{-1})g^{-1} \\ &= geg^{-1} \\ &= e\end{aligned}$$

Thus, $h^{-1}g^{-1}$ is an inverse for (gh). But since inverses are unique, it is *the* inverse for (gh). □

Now that we have some of the basics down, we can begin to look at more structures on, and within groups.

1.3. **Orders.** First, to get some notation out of the way: when dealing with a general group G, we often write the group operation as multiplication (i.e.: the group product of g and h is written as gh). To this end, if we want to multiply an element by itself multiple times, we use exponents, just as we do in multiplication. So the element $ggggg$ we would write as g^5. Similarly, the element $g^{-1}g^{-1}g^{-1}g^{-1}g^{-1}$ would be written as g^{-5}. In this manner, we see that g^0 should be the identity, e. So an expression like $g^4(h^2g^3)^{-1}gg^3h^2$ can be simplified to $gh^{-2}g^4h^2$. Note: unless the group is abelian, we cannot group all of the g and h together. The order of group multiplication matters. We also note that we have to adapt the notation for specific groups with different operations: if the group is $(\mathbb{Z}, +)$ for example, then $gh = g + h$, $g^{-1} = -g$, $e = 0$, and $g^n = ng$. Don't confuse "group multiplication" with "multiplication of numbers".

We now provide a few important definitions:

Definition 1.3. Group Order If G is a group, the *order* of G is the number of elements it contains, finite or infinite. The order of G is denoted $|G|$.

Thus, for some of our examples in section 2.1, $|\mathbb{Z}_6| = 6$, $|D_3| = 6$, and $|\mathbb{Z}|$ is infinite (or, if we remember our work in MAT246, we could say that $|\mathbb{Z}| = \aleph_0$).

Definition 1.4. Element Order Let G be a group, and let $g \in G$ be any element. The *order* of g is the smallest integer n such that $g^n = e$. If there is no such n, we say g has *infinite order.* As in the group case, the order of g is denoted $|g|$.

So looking back to our Cayley table for D_3, we see that $|R_{120}| = 3$, and $|H| = 2$. The in case of $(\mathbb{Z}, +)$, the order of 1 is infinite: if we keep adding 1 to itself over and over, we will never reach the identity, 0. It is also important to remember that the order is the *smallest* integer n such that $g^n = e$. For H in D_3, we see that $H^4 = (H^2)^2 = e^2 = e$, but 4 isn't the smallest number to do so, so it isn't the order of H.

Proposition 1.1. Let G be a finite group. Then for every $g \in G$, $|g|$ is finite.

Proof. First of all, if $g = e$, then $|g| = 1$. Suppose $g \neq e$, and consider the sequence $S = \{e, g, g^2, g^3, \ldots\}$. Since G is closed under the operation, and there are only finitely many elements of G, this means that some of the elements in S are the same. Suppose $g^m = g^k$ for some $m, k \in \mathbb{N}$, with $m > k$. This means that $g^{m-k} = e$. Thus, since we have that there is a finite number n for which $g^n = e$, and the order is defined to be the *smallest* number such that g raised to that power is e, this means that $|g| \leqslant n < \infty$. □

It is important to note that the converse to this theorem is false: if G is an infinite group, there can still be $g \in G$ which have *finite* order. As an example, consider $G = \mathrm{GL}(2, \mathbb{R})$, which is infinite. Let $A = \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}$. Computing powers, we see that $A^2 = -I$, meaning $A^4 = I$, and since it's the smallest power to do so, $|A| = 4$, even though it lives in an infinite group. The order of $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, however, is infinite $\left(\text{since } B^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\right)$ so $\mathrm{GL}(n, \mathbb{R})$ has both finite and infinite order elements.

2. Dihedral Groups, D_n

We now briefly expand on the work we did for D_3 and generalise to other polygons.

Consider a regular n-sided polygon, centred at the origin. We wish to consider the group of symmetries of this object, which we will call D_n. We know that function composition is associative, and that rotating 0 degrees (or radians) does not change anything, so it acts as an identity. First, to get a sense of how many there are, we apply the same combinatorial method as in D_3: number the vertices $1, 2, \dots, n$, and for the purposes of this exercise, let us number them increasing clockwise (i.e.: starting from vertex 1, vertex 2 is the one that immediately follows as we go clockwise from it, etc.) The first choice we have is where to send vertex 1, and there are n distinct choices for this. Once we have made this choice, we have two choices left to us: we can either leave the rest of the vertices in the same orientation as we started with (i.e.: with vertex 2 as the one immediately following 1 clockwise), or to flip about the axis through the new location for vertex 1 (i.e.: with vertex 2 as the one next to vertex 1, but in the counterclockwise direction; vertex n is now the one next to 1 in the clockwise direction). Hence, in total, there are $2n$ choices for symmetries, meaning $|D_n| = 2n$.

If we just move vertex 1 to another place, and don't flip, this is equivalent to rotating by some angle which is a multiple of $2\pi/n$. In total, there are obviously n rotations we can make, and since rotating it 0 degrees is equivalent to not changing anything, we see that R_0 acts as the identity. For D_n, the convention is define $r := R_{2\pi/n}$. This r generates all the other rotations by repeatedly composing with itself, and we can see that $|r| = n$, since $r^n = R_{2n\pi/n} = R_{2\pi} = R_0 = e$.

If one were to write out the Cayley Table for any D_n, we would find ourselves in the situation in D_3 (which we will not formally prove): the rotations, and reflexions about any axis form the totality of the symmetries, that composing any two gives you another one from the list, and that each symmetry has an inverse which "undoes" the change. We saw it for D_3, and Gallian does D_4; you are welcome to try it for other n choices.

As the dihedral groups are an excellent source of examples, we'll try to simplify how we look at them. We will not prove these facts, but leave them as potential exercises: Consider D_n for $n \geqslant 3$, let r be defined as the rotation by $2\pi/n$ radians, and let s be the reflexion through any specified axis (choose one ahead of time, and stick with it). We have $|r| = n$, and $|s| = 2$ (the latter easily seen because reflecting twice through the same axis leaves the object unchanged). The elements of D_n are exactly the ones in the following list:

$$D_n = \{e, r, r^2, r^3, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\} \tag{2}$$

Meaning that any element of D_n can uniquely be written as $s^i r^j$, with $i \in \{0, 1\}$, and $j \in \{0, 1, \dots, n-1\}$. For any such j, the relation $sr^j = r^{-j}s$ holds true (this can be proven by induction). Since $r^n = e$, this means that for any j, $r^{-j} = r^{n-j}$. So the exponents of the rotations work under addition modulo n.

One can use these relations to simplify long strings of symmetries; for example, in D_{10}:

$$sr^4(r^2sr^5)s = sr^{4+2}r^{-5}s^2 = sr^{6-5} = sr$$

3. Subgroups, Cyclic Groups

3.1. **Subgroups, Subgroup Tests.** The eagle-eyed reader may have noticed that in examples of groups given in section 2.1, there appeared to be smaller groups hiding inside of them. For example, in D_3, the subset $\{R_0, R_{120}, R_{240}\}$ forms a group under the same function composition. In $\mathbb{Z}_6$, all of the even numbers also form a group under addition modulo 6. $\mathbb{Z}_6$ is *not* a subgroup of $\mathbb{Z}$, however, as the former has addition modulo 6 as its operation, and the latter has just addition, so they have different operations. When we have a given group, and find subsets which are also groups under the operation, we called these subsets *subgroups*. More precisely:

Definition 3.1. Subgroup Let G be any group. If there exists a subset $H \subseteq G$ such that H is also a group under the operation on G, then we call H a *subgroup* of G. The conventional notation for H being a subgroup of G is $H \leqslant G$.

Gallian points out that if $H \subset G$, but $H \neq G$, and H is a subgroup, it's denoted $H < G$. These are called *proper subgroups* (since they are proper subsets of G). In these notes, we will generally

use the $\leqslant$ notation for proper subgroups as well (and make a written note if we want to emphasise that H is proper).
The first example of a subgroup, present in every group G, is the set $\{e\}$. One can easily check that this is a subgroup; it is called the *trivial subgroup*. Any subgroup $H \leqslant G$ which is not the trivial subgroup is called a *nontrivial subgroup*.
There are a number of essentially equivalent tests to apply to see if a given subset of a group is actually a subgroup.

Theorem 3.1. Two-Step Subgroup Test Let G be a group, and let $H \subseteq G$ be nonempty. H is a subgroup of G if the following two conditions hold

(1) For any $a, b \in H$, the product ab is also in H.
(2) For any $a \in H$, the inverse a^{-1} is also in H

Proof. Suppose the two conditions above hold for $H \subseteq G$. The first condition directly says that the group operation on G is also a binary operation on H; i.e.: when we take the product of two things in H, then we always stay inside of H. We say that H is *closed* under the operation. Since the operation is a group operation on G, we know then that it must be associative, and thus it's associative on H. So now we have an associative, binary operation on H, which is half of the things we need for a group.
The second condition says that H is closed under taking inverses. For any element of H, the inverse is also in H; when we combine this with the first property, this means that if $a \in H, a^{-1} \in H$, so $aa^{-1} = e \in H$. Thus, H has an associative binary operation, an identity for that operation, and every element of H has an inverse under the operation. Thus, by definition, H is a group. □

We can actually cut down our work by half when checking for subgroups, with the following test

Theorem 3.2. One-Step Subgroup Test Let G be a group, and $H \subseteq G$ nonempty. H is a subgroup of G if the following condition holds

(1) $ab^{-1} \in H$ for *any* $a, b \in H$

Proof. As last time, we know that the group operation on G must be associative. Now, let $h \in H$ be any element. From the above condition, let $a = h$, and $b = h$. Since ab^{-1} has to be in H, this means that $h(h^{-1}) = e$ is in H. So now we can cleverly choose a, b to show that H contains the inverses of all its elements: let $a = e$, and let $b = h$ for any $h \in H$. By the above condition, this means that $ab^{-1} = eh^{-1} = h^{-1} \in H$. So H is closed under inverses. Now we just have to show that H is closed under the operation it inherits from G. Let h_1, h_2 be any elements of H. Since H is closed under inverses, this means that $h_2^{-1} \in H$. So let $a = h_1, b = h_2^{-1}$. Thus, by the condition, we have

$$ab^{-1} = h_1(h_2^{-1})^{-1} = h_1 h_2 \in H$$

So H is closed under the operation on G. Thus, it satisfies all the properties of a group, meaning $H \leqslant G$. □

One of the important things to remember to check first is that the subset H you are given is actually nonempty. If one has a finite group, then there is another test one can apply.

Theorem 3.3. Finite Group Subgroup Test Let G be a finite group. Let $H \subseteq G$ be a nonempty subset of G. If the operation of G is also a binary operation on H (i.e.: H is closed under the group operation on G), then H is a subgroup of G.

Proof. H is nonempty, and closed under the operation, which is a good start. From the two-step subgroup test, we just need to check that H is closed under inverses, i.e.: that for all $h \in H$, h^{-1} is also in H. Let h be any element of H. From proposition 2.1, we know that $|h| < \infty$, since G

is finite. Define $n := |h|$. Then this means that $h(h^{n-1}) = e$, giving $h^{-1} = h^{n-1}$, and $h^{n-1} \in H$ since H is closed under the operation. Hence, H is closed under inverses, and so by the two-step subgroup test, must be a subgroup of G. □

This really only works for finite groups. As a counterexample, consider the group $G = (\mathbb{Q}^*, \times)$, the non-zero rationals under multiplication. Let H be the odd nonzero integers. Odd numbers are certainly closed under multiplication, but H does not contain any inverses (since, for example, $3 \in H$, but $1/3 \notin H$), so H is not a subgroup of G.
Now let us use these tests to find some subgroups.
Examples

(1) Let $G = \mathbb{Z}_8$ under addition modulo 8. Let $H = \{0, 2, 4, 6\} \subset G$. Obviously H is nonempty. For any $x \in \mathbb{Z}_8$, the inverse is $x^{-1} = -x \mod 8 = (8 - x)$. Let $2n$ and $2m$ be elements of H (since they're all even). Then $(2m)^{-1} = -2m$. Thus, "ab^{-1}" $= (2n-2m) \mod 8 = 2(n-m) \mod 8$, which must also be in H. Thus, by the one step subgroup test, H is a subgroup.

(2) Let $G = \mathrm{GL}(2, \mathbb{R})$. Let $H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \neq 0 \right\}$. We want to determine if this is a subgroup of G. First of all, we know that H is nonempty, because $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is in H. Let $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, and $B = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$ be matrices in H. This means that $B^{-1} = \begin{pmatrix} 1/c & 0 \\ 0 & 1/d \end{pmatrix}$. The we see that $AB^{-1} = \begin{pmatrix} a/c & 0 \\ 0 & b/d \end{pmatrix}$, and this must also be in H, since neither a/c nor b/d is 0, and the result is still diagonal. Thus H is a subgroup of G.

(3) Let $G = \mathbb{C}^*$, the nonzero complex numbers under multiplication. If $z = a + bi \in \mathbb{C}^*$, then $(a+bi)^{-1}$ is the number such that $(a+bi)(a+bi)^{-1} = 1$; thus, $(a+bi)^{-1} = (a-bi)/(a^2+b^2)$. Let $H = \{a + bi \in \mathbb{C}^* \mid a^2 + b^2 = 1\}$. Firstly, we notice that H is nonempty, since $1 \in H$. Let $a+bi, c+di \in H$. Then consider $(a+bi)(c+di)^{-1} = (a+bi)(c-di)/(c^2+d^2)$. But since $c^2 + d^2 = 1$, this means we have $(a + bi)(c + di)^{-1} = (ac + bd) + (bc - ad)i$. To determine if this is in H, we need to see if it satisfies the property of everything in H:

$$\begin{aligned}(ac + bd)^2 + (bc - ad)^2 &= a^2c^2 + b^2d^2 + 2acbd + b^2c^2 + a^2d^2 - 2adbc \\ &= a^2(c^2 + d^2) + b^2(c^2 + d^2) \\ &= a^2 + b^2 \\ &= 1\end{aligned}$$

Thus, for any $a + bi, c + di \in H$, we have $(a + bi)(c + di)^{-1} \in H$, meaning H is a subgroup of G. Geometrically, H is the unit circle centred at 0 in the complex plane.

(4) Let $G = D_5$. Let $H = \{e, r, r^2, r^3, r^4\}$, all of the rotations (which is clearly nonempty). For any $r^j \in H$, $(r^j)^{-1} = r^{-j}$, with the exponents operating under addition mod5. Let $r^j, r^k \in H$, then $r^j(r^k)^{-1} = r^{j-k} \in H$, and so by the one-step subgroup test, $H \leqslant G$.

(5) Let G be any abelian group. Let $H = \{x \in G \mid x^2 = e\}$. We notice that H is nonempty, since $e^2 = e$, so $e \in H$. If $h^2 = e$, this means that $h^{-1} = h$. Let $h_1, h_2 \in H$, so $h_1^2 = e$, $h_2^2 = e$. Then $h_1(h_2)^{-1} = h_1h_2$. We need to check if this is in H, i.e.: if it squares to the identity.

$$(h_1h_2)^2 = h_1h_2h_1h_2 = h_1h_1h_2h_2 = (h_1)^2(h_2)^2 = ee = e$$

Where we used the abelian-ness of G to exchange the middle h_2h_1 above to be h_1h_2. Hence $h_1h_2^{-1} \in H$, so H is a subgroup of G.

Now that we've seen some examples of subsets which *are* subgroups, let's look at some subsets which are not. For a subset to fail to be a subgroup, it only has to fail one of the properties of being a

group: not containing the identity, not being closed under the operation, etc.
Examples

(1) Let $G = \mathbb{Z}$, let $H = \mathbb{Z}^+$, the set of positive integers. H fails to be a subgroup because it does not contain the identity 0. It also fails because none of the elements of H have inverses also in H (since the additive inverse of $x \in \mathbb{Z}$ is $-x$).
(2) Let $G = \mathbb{Q}^*$ under multiplication. The subset $H = \mathbb{Z}^* \subset \mathbb{Q}^*$ is not a subgroup, since it is not closed under inverses: in $\mathbb{Q}^*$, the inverse of x is $1/x$. So $2 \in \mathbb{Z}^*$, but $2^{-1} = 1/2 \notin \mathbb{Z}^*$
(3) Let $G = D_{10}$, and let H be the odd powers of the r: $H = \{r, r^3, \ldots, r^9\}$. H fails to be a subgroup since it does not contain the identity, e. It also is not closed under the operation, since $rr = r^2 \notin H$.

3.2. Some Common Examples of Subgroups.

Definition 3.2. Centre Let G be any group. The *centre of* G is defined to be the elements of G which commute with all other elements of G. Formally,

$$Z(G) := \{x \in G \,|\, xg = gx \;\forall\, g \in G\}$$

Every group has a centre, though some groups centres may be trivial (i.e.: only contains the identity element).

Proposition 3.1. For any group G, the centre $Z(G)$ is a subgroup of G.

Proof. $Z(G)$ is nonempty, since the identity trivially commutes with everything: $eg = ge (= g)$ for all $g \in G$. Let $x, y \in Z(G)$. This means that for any $g \in G$, we have $xg = gx$, and $yg = gy$. So now the question is, is $(xy) \in Z(G)$? Let g be any element of G. Then we see that

$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$$

meaning (xy) commutes with all elements of G. Hence, $Z(G)$ is closed under the operation of G. Secondly, we notice is that if $yg = gy$, then if we multiply on the left *and* right by y^{-1}, we get $gy^{-1} = y^{-1}g$. More carefully:

$$\begin{array}{cccc} yg = gy & \Rightarrow & y^{-1}(yg) & = & y^{-1}(gy) \\ & \Rightarrow & y^{-1}(yg)y^{-1} & = & y^{-1}(gy)y^{-1} \\ & \Rightarrow & (y^{-1}y)gy^{-1} & = & y^{-1}g(yy^{-1}) \\ & \Rightarrow & gy^{-1} & = & y^{-1}g \end{array}$$

Since this is true for any $g \in G$ this means if $y \in Z(G)$, then $y^{-1} \in Z(G)$. Hence, the centre is closed under inverses. Hence, by the two-step subgroup test, $Z(G) \leqslant G$. □

Examples:

(1) Let $G = Z_6$. G is abelian, which means everything commutes with everything else, and hence $Z(G) = G$.
(2) Let $G = D_n = \{e, r, r^2, \ldots r^{n-1}, s, sr, sr^2, \ldots sr^{n-1}\}$. We want to compute the elements which commute with everything. As we know, a generic element of D_n can be written as $s^i r^j$, where i is 0 or 1, and j can range from 0 to $(n-1)$. So we need all the $g \in D_n$ such that $g(s^i r^j) = (s^i r^j)g$ for all $s^i r^j$. Now we need to be careful to not get lost in notation: since $g \in D_n$, this means that $g = s^k r^\ell$ for some k, ℓ in the appropriate ranges. Now we need to solve

$$s^k r^\ell (s^i r^j) = (s^i r^j) s^k r^\ell$$
$$\Rightarrow s^{k+i} r^{j-\ell} = s^{k+i} r^{\ell-j}$$

But we need to remember: i, j can range over all possibilities. It's the k, ℓ that we need to figure out; we need the k, ℓ which makes the above true for all i, j. If we use the cancellation

law above to get rid of the s^{k+i}, we need to solve $r^{j-\ell} = r^{\ell-j} = (r^{j-\ell})^{-1}$, for any j. Specifically, when $j = 0$, this reduces to $r^{\ell} = r^{-\ell}$ (since it has to be true for all j in the range, it certainly has to be true when $j = 0$). Since we know that $r^{-\ell} = r^{n-\ell}$, this means that we need $\ell = n - \ell$, or rearranging, $\ell = n/2$. Hence, it only has a nonzero solution when n is even, and no solution when n is odd (other than $\ell = 0$).
Now we've dealt with the r^j part of g, what about the s^k? Well, the only options are $k = 0$ or $k = 1$. If $k = 0$, and $j = 0$, then we're left with $g = s$. But $s(r) = r^{-1}s \neq rs$, so $s \notin Z(D_n)$. If $k = 0$, and $j = n/2$ (for n even), then $g = r^{n/2}$, and we see:

$$r^{n/2}(s^i r^j) = s^i r^{j-n/2} = s^i r^{j+n/2} = (s^i r^j) r^{n/2}$$

(the middle equality works because the exponents are adding in addition modulo n; check that $x + n/2 \mod n \equiv x - n/2 \mod n$ for any x). So $r^{n/2}$ is in $Z(D_n)$ if n is even. So the only case we have left to check is $sr^{n/2}$. But here we get a bit crafty: We know that $Z(D_n)$ is a subgroup of D_n, and we also know that $r^{n/2}$ is in it. If $sr^{n/2}$ were also in it, then the product of the two would be in it: namely, $sr^{n/2}r^{n/2} = sr^n = s$. But we know s isn't in it, meaning $sr^{n/2}$ cannot be in $Z(D_n)$. Thus, we conclude:

$$Z(D_n) = \begin{cases} \{e, r^{n/2}\} \; n \,\text{even} \\ \{e\} \; n \,\text{odd} \end{cases}$$

Proposition 3.2. Let G be any group. Then G is abelian if and only if $Z(G) = G$.

We leave the proof as a (brief) exercise, since it follows immediately from the definitions.
The centre of G looks at the elements which commute with *everything* in G; what if we wanted to look at things that commute with a smaller subset of G? For example, a single element?

Definition 3.3. Centraliser Let G be a group, and let $g \in G$. The *centraliser of* g is the set of all elements of G which commute with g. Formally,

$$C(g) := \{x \in G \mid xg = gx\}$$

Unsurprisingly, we have the following

Proposition 3.3. Let G be a group, and let $g \in G$. The centraliser, $C(g)$ is a subgroup of G.

Proof. This is the same as the previous proposition. $C(g)$ is nonempty, since $eg = ge = g$ for any g. Secondly, if $x, y \in C(g)$, then $(xy) \in C(g)$ since $(xy)g = x(yg) = x(gy) = (xg)y = g(xy)$. Lastly, if $x \in C(g)$, then $x^{-1} \in C(g)$ as $xg = gx$ gives $gx^{-1} = x^{-1}g$ by multiplying left and right by x^{-1}. Thus, $C(g) \leqslant G$. □

Corollary 3.1. Let G be a group. If $g \in Z(G)$, then $C(g) = G$.

Again, this follows nearly directly from the definitions, and so is left as an exercise.
Examples

(1) Let $G = \mathbb{Z}_{10}$, let $g = 2$. Well, G is abelian in this case, so $C(2) = \mathbb{Z}_{10}$.

(2) Let $G = D_4$, let $g = r$. $C(r) = \{x \in D_4 \mid xr = rx\}$. Since x is of the form $s^i r^j$ with i being 0 or 1, and $j \in \{0, 1, 2, 3\}$, the condition is then $r(s^i r^j) = (s^i r^j)r$. Simplifying when $i = 1$, we get $sr^{j-1} = sr^{j+1}$. Cancelling the s we're left with $r^{j-1} = r^{j+1}$, meaning we need to solve $j + 1 \equiv (j - 1) \mod 4$. If we check all $j = 0, 1, 2, 3$, we see that there is no solution. So looking at the case when $i = 0$, we have $rr^j = r^j r$, but since both are equal to r^{j+1}, this means that r^j for all $j = 0, 1, 2, 3$ satisfy this. Hence, $C(r) = \{e, r, r^2, r^3\}$

(3) Let $G = \mathrm{GL}(2,\mathbb{R})$. Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. $C(A) = \{B \in \mathrm{GL}(2,\mathbb{R}) \,|\, AB = BA\}$. Let $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Writing this out:

$$1) \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$$

$$2) \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$$

Equating the two, we see that $d = c + d$, meaning $c = 0$. We also see that $a + b = b + d$, and so $a = d$. As the determinant cannot be zero, this means $a \neq 0$. Since there are no further restrictions, this means we can conclude

$$C\Big(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \Big) = \Big\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \,\Big|\, a, b \in \mathbb{R},\, a \neq 0 \Big\} \subset \mathrm{GL}(2,\mathbb{R})$$

3.3. **Cyclic Groups and Subgroups.** In this section, we introduce one of the important classes of subgroups (and groups). Let G be any group, and let $g \in G$ be any element. We use $\langle g \rangle$ to denote the set of all repeated multiples of g with itself and with its inverse. Formally,

$$\langle g \rangle = \{\, g^n \,|\, n \in \mathbb{Z}\} = \{e, g, g^{-1}, g^2, g^{-2}, \ldots\} \tag{3}$$

The set $\langle g \rangle \subseteq G$ is called the *cyclic subgroup generated by g*, because of the wonderful fact that

Proposition 3.4. The set $\langle g \rangle \subseteq G$ is a subgroup of G

Proof. We know that $g \in \langle g \rangle$, so it is nonempty. Let $x, y \in \langle g \rangle$, which means $x = g^n$, $y = g^k$ for some $n, k \in \mathbb{Z}$. Then $xy^{-1} = g^n g^{-k} = g^{n-k} \in \langle g \rangle$, since $(n - k) \in \mathbb{Z}$. Thus, by the one step subgroup test, $\langle g \rangle \leqslant G$. □

Examples

(1) Let $G = \mathbb{Z}_{12}$. Then $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$, since in an additive group, g^n means ng. We also see that $\langle 1 \rangle = \mathbb{Z}_{12}$.

(2) For the full integers $G = \mathbb{Z}$, we see $\langle 1 \rangle = \mathbb{Z}$, as $\langle 1 \rangle = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$. But also, $\langle -1 \rangle = \mathbb{Z}$, as $\langle -1 \rangle = \{0, -1, 1, -2, 2, -3, 3, \ldots\}$. The subgroup $\langle 2 \rangle = \{0, 2, -2, 4, -4, \ldots\}$ is all of the even integers, denoted $2\mathbb{Z}$.

(3) Let $G = D_n$, and let $r = R_{360/n}$ (the rotation that sends vertex i to vertex $i + 1$). Then we see that $\langle r \rangle = \{e, r, r^2, r^3, \ldots, r^{n-1}\}$, which is the set of all rotations. $\langle r \rangle \subset D_n$ is called the rotation subgroup.

(4) Let $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$. This means $A^{-1} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$. One can easily show with induction that $A^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}$ for any $n \in \mathbb{Z}$. This means that $\langle A \rangle = \Big\{ \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \,\Big|\, n \in \mathbb{Z} \Big\}$.

Theorem 3.4. Let G be any group, and let $g \in G$.

(1) If g has infinite order, then $g^k = g^m$ if and only if $k = m$.

(2) If g has finite order, $|g| = n$, then $\langle g \rangle = \{e, g, g^2, g^3, \ldots, g^{n-1}\}$, and $g^i = g^j$ if and only if n divides $i - j$.

Proof. (1) If $|g|$ is infinite, then $g^n = e$ has no nonzero solution for $n \in \mathbb{Z}$. Thus, if $g^k = g^m$, this means $g^{k-m} = e$, so $k - m = 0$, giving $k = m$. Conversely, if $k = m$, then clearly $g^k = g^m$.

(2) If $|g| = n$, finite, then we know $S := \{e, g, g^2, \ldots, g^{n-1}\}$ must be distinct: since n is the *smallest* positive number such that $g^n = e$, then if $g^i = g^j$ for both $i, j < n$, we'd have $g^{i-j} = e$, with $i - j < n$,

which is a contradiction. Now let g^k be any element of $\langle g\rangle$ with $k > n$ (otherwise, $g^k \in S$). By the division algorithm, we know there exists $q, r \in \mathbb{Z}$ with $0 \leqslant r < n$ such that $k = qn + r$. This means

$$g^k = g^{qn+r} = (g^n)^q g^r = eg^r = g^r \ \in \ S$$

since $r < n$. Hence $\langle g\rangle = S = \{e, g, g^2, \ldots, g^{n-1}\}$.
Now, suppose for $i, j \in \mathbb{Z}$, we have $n|(i-j)$; i.e.: there is a $q \in \mathbb{Z}$ such that $(i-j) = qn$. Then $g^{i-j} = g^{nq} = (g^n)^q = e$, and so $g^i = g^j$.
Conversely, suppose $g^i = g^j$, implying $g^{i-j} = e$. Again by the division algorithm, that $\exists q, r \in \mathbb{Z}$ with $0 \leqslant r < n$ such that $(i-j) = qn + r$. This gives us

$$e = g^{i-j} = g^{qn+r} = (g^n)^q g^r = eg^r = g^r$$

But since $r < n$, and since n is the smallest positive integer such that $g^n = e$, this means $r = 0$. In other words, $(i-j) = qn + 0$, meaning $n|(i-j)$. □

And now we see the reason for using $|\cdot|$ to mean "order", in terms of both groups and elements:

Corollary 3.2. Let G be a group, and let $g \in G$. Then $|g| = |\langle g\rangle|$

There is another quick corollary of the theorem which is very useful:

Corollary 3.3. Let G be a group, and let $g \in G$. If $g^k = e$, then $|g|$ divides k.

Proof. This is a special case of the theorem above, for $i = k, j = 0$. If $g^k = e = g^0$, then by the theorem we know that $|g|$ divides $k - 0 = k$. □

We saw for $G = (\mathbb{Z}, +)$, we had both $\mathbb{Z} = \langle 1\rangle$, and $\mathbb{Z} = \langle -1\rangle$. If we look at another example, say $G := \{e, x, x^2, x^3, x^4\}$, under multiplication with $x^5 = e$, we clearly see that $\langle x\rangle = G$. But if we consider $\langle x^3\rangle$, we see

$$\begin{aligned}\langle x^3\rangle &= \{e, x^3, (x^3)^2, (x^3)^3, (x^3)^4, \ldots\}\\ &= \{e, x^3, x^6, x^9, x^{12}, x^{15}, x^{18}, \ldots\}\end{aligned}$$

But since the exponents act as addition modulo 5 (the order of x), we see $x^6 = x^5x = ex = x$. And $x^9 = x^5x^4 = x^4$. Continuing like this, we see $\langle x^3\rangle = \{e, x, x^2, x^3, x^4\} = G$, meaning G has x as a generator, but it also has x^3 as a generator.
We would like to know, generally, how many different elements of a cyclic group $\langle g\rangle$ also generate the whole group, and the following theorem helps us with that

Theorem 3.5. Let G be any group, with $g \in G$, and $k \in \mathbb{Z} \setminus \{0\}$.

(1) If $|g| = \infty$, then $|g^k| = \infty$.
(2) If $|g| = n < \infty$, and $k \in \mathbb{N}$, then $\langle g^k\rangle = \langle g^{\gcd(n,k)}\rangle$
(3) If $|g| = n < \infty$, then $|g^k| = \frac{n}{\gcd(n,k)}$

Proof. (1) Suppose $|g| = \infty$, but $|g^k| = m < \infty$. This means that $e = (g^k)^m = g^{km}$. We also see that $g^{-km} = (g^{km})^{-1} = e^{-1} = e$. Since neither k, nor m is 0, this means one of $\pm km$ is positive. But this would imply there exists a positive integer such that g to that power is the identity, contradicting the supposition that $|g| = \infty$. This $|g^k| = \infty$
(2) Let $d := \gcd(n, k)$. Since d divides k, we can write $k = dr$ for some $r \in N$. Thus, $g^k = (g^d)^r$, which means that $\langle g^k\rangle \subseteq \langle g^d\rangle$ (if you write out all of the elements of $\langle g^d\rangle$, the elements of $\langle g^k\rangle$ will appear since k is a multiple of d). Since $d := \gcd(n, k)$, we know that there are integers x, y such that $d = xk + yn$ (the "GCD Theorem"). Thus, we see

$$g^d = g^{xk+yn} = g^{xk}g^{yn} = (g^k)^x(g^n)^y = (g^k)^x e^y = (g^k)^x \ \in \ \langle g^k\rangle$$

So since $g^d \in \langle g^k \rangle$, this means that $\langle g^d \rangle \subseteq \langle g^k \rangle$ by closure.
Thus, $\langle g^d \rangle \subseteq \langle g^k \rangle$, and $\langle g^k \rangle \subseteq \langle g^d \rangle$, meaning $\langle g^d \rangle = \langle g^k \rangle$.
(3) This is really a corollary of part (2). If $\langle g^d \rangle = \langle g^k \rangle$, then $|\langle g^d \rangle| = |\langle g^k \rangle|$. Since the order of the cyclic group generated by an element *is* the order of that element, we have $|g^k| = |g^{\gcd(k,n)}|$. □

So what this tells us is that if we have a finite cyclic group $G = \langle g \rangle$, then the other powers of g that generate the whole group are the powers which are relatively prime to $|g|$. Formally,

Corollary 3.4. *Let $G = \langle g \rangle$ be a finite cyclic group, with $|g| = n$. Then $\langle g^k \rangle = G$ if and only if $\gcd(n,k) = 1$.*

Ex.: Let $G = \mathbb{Z}_n$, which is a cyclic group of order n generated by the element 1, i.e.: $\mathbb{Z}_n = \langle 1 \rangle$. The other elements $k \in \{0, 1, \ldots, n-1\}$ such that $\langle k \rangle = \mathbb{Z}_n$ are the ones such that $\gcd(k,n) = 1$.

What this means is that if we have a cyclic group, and we know one of the generators, then we can figure out *all* of the generators.
As an example, let us consider $G = \langle x \rangle$, where $|G| = |x| = 24$. This means $G = \{e, x, x^2, \ldots, x^{23}\}$. If we want to find all of the generators of G, we must find the x^k such that $\gcd(k, 24) = 1$. The prime decomposition of 24 is $2^3 \cdot 3$, so the prime decomposition of k cannot have any of these primes. Thus, we see the possibilities are:

$$k = \{1, 5, 7, 11, 13, 17, 19, 23\}$$

So $G = \langle x \rangle = \langle x^5 \rangle = \langle x^{17} \rangle$, etc.

Theorem 3.6. Fundamental Theorem of Cyclic Groups *Let G be a cyclic group.*

1. *Every subgroup H of G is also cyclic.*
2. *If $|\langle x \rangle| = n$, for $x \in G$, then for any subgroup $H \leqslant \langle x \rangle$, $|H|$ divides n; if k is a divisor of n, then there is one subgroup of $\langle x \rangle$ of order k, namely $\langle x^{n/k} \rangle$*

Proof. (1) Let G be a cyclic group, generated by x: $G = \langle x \rangle$. Let H be a subgroup of G: if $H = \{e\}$, then it is clearly cyclic. So let $H \neq \{e\}$. Since $H \subset G$, this means every element of H is of the form x^j, for $j \in \mathbb{Z}$. Since H is a subgroup, if $x^i \in H$, then $x^{-i} \in H$. Thus, one of $\pm i$ must be a positive integer, so H contains an element which is a positive power of x. Now, let m be the smallest positive integer such that $x^m \in H$. This implies that $\langle x^m \rangle \subseteq H$, by the closure of the group operation.
Claim: $H = \langle x^m \rangle$. To prove this to be true, we must show that for any $y \in H$, $y \in \langle x^m \rangle$. So let y be any element of H; since $y \in G$ as well, this means $y = x^j$ for some $j \in \mathbb{Z}$. We can use the division algorithm to write $j = mq + r$ with $0 \leqslant r < m$. This means that $x^j = x^{mq+r} = x^{mq}x^r$. We can re-arrange to get $x^r = x^j x^{-mq}$, and since both $x^j \in H$, and $(x^m)^{-q} \in H$, then $x^r \in H$ by closure. But m was the least positive integer such that x^m is in H, and we know $r < m$. This is a contradiction, so r must be 0, meaning $x^j = (x^{mq}) \in \langle x^m \rangle$. Thus $H \subseteq \langle x^m \rangle$, but since $\langle x^m \rangle \subseteq H$, this means they must be equal. Thus, any $H \leqslant G = \langle x \rangle$ is also cyclic.
(2) Suppose $|\langle x \rangle| = n$, and let $H \leqslant \langle x \rangle$ be any subgroup. We know from (1) that $H = \langle x^m \rangle$ where m is the least positive integer such that $x^m \in H$. If we let $y = e = x^n$, then we get $n = mq$ from the previous analysis. Since $|H| = |\langle x^m \rangle| = n/\gcd(n,m) = mq/\gcd(mq,m) = mq/m = q$, this means that $|H|$ divides $|\langle x \rangle|$.
Lastly, for any k dividing n, $|\langle x^{n/k} \rangle| = n/\gcd(n, n/k) = n/(n/k) = k$. So certainly $\langle x^{n/k} \rangle$ is a subgroup of $\langle x \rangle$ of order k. To show it is the only one, suppose H is any subgroup of $\langle x \rangle$ with $|H| = k$. From (1), we know $H = \langle x^m \rangle$ where m is the least positive integer such that $x^m \in H$, and $m|n$. This means that $m = \gcd(n,m)$, and

$$k = |x^m| = |x^{\gcd(n,m)}| = n/\gcd(n,m) = n/m$$

Meaning $m = n/k$, i.e.: $H = \langle x^m \rangle = \langle x^{n/k} \rangle$.

□

So going back to our example of $G = \langle x \rangle$ with $|G| = 24$, we can tell from the preceding theorem that the subgroups of G are of the form $\langle x^m \rangle$ where m divides 24. Also, if k divides 24, then we know that the subgroup of order k must be $\langle x^{24/k} \rangle$. Using this knowledge, we can list the subgroups:

$$\begin{array}{rcc c}
\langle x \rangle & = & \{e, x, x^2, \ldots, x^{23}\} & \text{order } 24 \\
\langle x^2 \rangle & = & \{e, x^2, x^4, \ldots, x^{22}\} & \text{order } 12 \\
\langle x^3 \rangle & = & \{e, x^3, x^6, x^9, \ldots, x^{21}\} & \text{order } 8 \\
\langle x^4 \rangle & = & \{e, x^4, x^8, x^{12}, x^{16}, x^{20}\} & \text{order } 6 \\
\langle x^6 \rangle & = & \{e, x^6, x^{12}, x^{18}\} & \text{order } 4 \\
\langle x^8 \rangle & = & \{e, x^8, x^{16}\} & \text{order } 3 \\
\langle x^{12} \rangle & = & \{e, x^{12}\} & \text{order } 2 \\
\langle x^{24} \rangle & = & \{e\} & \text{order } 1
\end{array}$$

This is all of the subgroups of G; using theorem 4.5, we can see which other elements generate any given subgroup. For example, $\langle x^3 \rangle = \langle x^9 \rangle$, since $\gcd(9, 24) = 3$.

Corollary 3.5. Let $G = \mathbb{Z}_n$. The subgroup $\langle n/k \rangle$ is the unique subgroup of order k, and these are the only subgroups of $\mathbb{Z}_n$.

(This is almost a non-corollary, as we will see when we get to isomorphisms.)

4. Permutation Groups

We revisit an important example we saw back in section 2: Let X be a set. A *permutation* of X is a function $f : X \to X$ which is a bijection.

Proposition 4.1. Let X be a set. The collection of all permutations of X forms a group under function composition, called the *Symmetric Group.*

Proof. We already proved this, section 2 example 10. □

We'll generally be dealing with X being a finite set, though in principle we can consider the permutations of any set. For a set X of size $n \in \mathbb{N}$, the convention is to label the elements as $X = \{1, 2, 3, \ldots, n\}$; in this case, we call the group of permutations on X the "symmetric group on n elements", and denote it S_n. We define a permutation on how it acts on individual elements. For example, if $X = \{1, 2, 3, 4, 5\}$, we can consider the permutation $f : X \to X$, defined by:

$$f(1) = 2 \qquad f(2) = 3 \qquad f(3) = 5 \qquad f(4) = 4 \qquad f(5) = 1$$

We can also consider the permutation $g : X \to X$ defined by:

$$g(1) = 1 \qquad g(2) = 5 \qquad g(3) = 4 \qquad g(4) = 2 \qquad g(5) = 3$$

Now, we can look at the permutation we get by composing f and g together. First, let us consider $g \circ f$, which means we take an element of X, act f on it, and then act g on the result. So for example, $(g \circ f)(1) = g(f(1)) = g(2) = 5$; in mapping notation, $1 \xrightarrow{f} 2 \xrightarrow{g} 5$. By computing all of the possibilities, we can see

$$(g \circ f)(1) = 5 \qquad (g \circ f)(2) = 4 \qquad (g \circ f)(3) = 3 \qquad (g \circ f)(4) = 2 \qquad (g \circ f)(5) = 1$$

Notice that while $(g \circ f)(1) = 5$, $(f \circ g)(1) = f(g(1)) = f(1) = 2$. So $f \circ g \neq g \circ f$ in this case, meaning that we can conclude not all permutation groups are abelian.

4.1. **Cycle Notation.** (Note: While Gallian introduces an intermediary notation for permutations, I feel it's easier to just skip ahead to cycle notation as it is the only real notation we will be using for our examples and exercises; having two similar-looking but differently-interpreted notations feels a bit confusing and cumbersome, though feel free to read through the appropriate subsection of Gallian)

Cycle notation is much more efficient way of describing the permutations of a given set, and allows for a very easy method for computing the composition of two permutations. Let us go back to the example we saw for $X = \{1, 2, 3, 4, 5\}$, the permutation f: 1 is send to 2, 2 is then sent to 3, 3 is sent to 5, and 5 is sent back to 1; the element 4 is fixed. The way we can represent this is as follows:

$$f = (1235)(4)$$

What this tells us is that inside any set of parentheses ( ), the permutation f sends any element listed to the element listed directly to the right of it; when you get to the end of the list, it goes back to the start. If only one element is listed inside, like (4), this means that element is fixed. (We will get to the point where we no longer write fixed elements). Let's look at some more examples:

Examples

(1) Again for X with five elements, we saw g, and $g \circ f$ above. Writing them in cycle notation, we have

$$g = (2534)(1), \qquad (g \circ f) = (15)(24)(3)$$

(2) Let $X = \{1, 2, 3, 4, 5, 6\}$, and let the permutation σ be defined as

$$\sigma(1) = 3 \qquad \sigma(2) = 4 \qquad \sigma(3) = 5 \qquad \sigma(4) = 2 \qquad \sigma(5) = 6 \qquad \sigma(6) = 1$$

Then we can write $\sigma = (1356)(24)$

One of the things we notice is that for a given permutation, we can "rotate" the elements inside a set of parentheses and not change the permutation. for example, if $\sigma = (1356)$, then we can push everything to the right one element (moving the last one to the first position) to get (6135), and it is the same permutation: 1 still goes to 3, 3 to 5, 5 to 6, 6 to 1. Hence $\sigma = (1356) = (6135) = (5613) = (3561)$. We *cannot*, however, mix up the order of the elements. So if $\sigma = (1356)$, then $\sigma \neq (1365)$, since the former sends 3 to 5, but the latter sends 3 to 6.

For a given permutation (of a given set), since all of the elements contained in one set of parentheses cycle through one another, we call such a collection a *cycle*, and we denote it by the number of elements inside of it: for one of the form $(x_1 x_2 \cdots x_n)$, we call it an *n-cycle*. So for the example above, $\sigma = (1356)(24)$, the part (1356) is a 4-cycle, and (24) is a 2-cycle. A 1-cycle merely fixes an element, so we will often omit them from our notation: thus, if τ is a permutation of the set of eight elements, and $\tau = (145)(6)(28)(3)(7)$, we will simply write $\tau = (145)(28)$.

4.2. **Composing Cycles.** Cycle notation allows us to quickly figure out what the composition of two permutations is, though it can take a little getting used to at first. The best way to start is with some explicit worked examples:

(1) Let $X = \{1, 2, 3, 4, 5\}$, and σ, τ permutations of X with $\sigma = (1435)$, $\tau = (231)$, and we want to know what permutation we get by composing $\sigma \circ \tau$. For convenience, and to put ourself more in line with the notation we introduced for general groups, we will write $\sigma \circ \tau = \sigma\tau$. This is a permutation we get by taking an element of X, first applying τ, and then applying σ to the result; this means we will be reading right to left. So to begin:

$$\sigma\tau = (3425)(231)$$

We can start with any element (number), but for the sake of convenience and ease, we usually start with the smallest number first, and work upwards. So the smallest number to

appear is 1; since we're reading right to left, the first cycle 1 appears in is (231), and 1 is sent to 2. Now we want to see where 2 is sent to, but we don't stay in the same cycle, we move along the cycles to the left. In the adjacent cycle, 2 appears and is sent to 5, so in the combination $1 \mapsto 2 \mapsto 5$, the total mapping is $\sigma\tau(1) = 5$. Now we start over to see where 5 is sent, but beginning from the far right, we see 5 only appears in (3425), meaning 5 is sent to 3. So $\sigma\tau(5) = 3$. Now we begin again with 3, and see it appears first in (231), showing 3 is mapped to 1. The number 1 does not appear to the left of that cycle, so the mapping is given by $\sigma\tau(3) = 1$. So the first part of the cycle $\sigma\tau$ we have is (153).
So now that we know where 1,5, and 3 are sent, we start the entire process again, generating a new cycle, with the next smallest number. In our case, this is 2: in the right-most cycle, 2 is sent to 3; moving left, 3 is sent to 4. So $\sigma\tau(2) = 4$. Lastly, 4 only appears in (3425), and this shows that 4 is sent to 2. Thus, the second part of the cycle is (24). We have now exhausted all of our numbers, leading us to conclude that $\sigma\tau = (153)(24)$.

(2) let $X = \{1, 2, 3, 4, 5, 6, 7\}$, and let σ, τ be permutations of X, such that $\sigma = (2376)(15)$, $\tau = (15634)(27)$, and we want to know what permutation we get by composing $\sigma \circ \tau$. We write the composition by writing out the cycles in order, and then simplifying after. So to begin:

$$\sigma\tau = (2376)(15)(15634)(27)$$

and we keep in mind that τ acts first, meaning we read right to left. The smallest number to appear is 1; since we're reading right to left, the first cycle 1 appears in is (15634), and in this cycle, 1 is sent to 5. Now we move along the cycles leftwards, to see where 5 goes, and we see the next cycle in which it appears is (15), meaning 5 is then sent to 1. Moving even further to the left, we see 1 isn't sent anywhere else, so the pattern is $1 \mapsto 5 \mapsto 1$. So the cycle (1) will appear in the composition.
Next we move on to 2, and see it appears in the first cycle from the right, (27), meaning 2 is sent to 7. We move along the cycles to the left, and notice the next cycle that 7 appears in is (2376), meaning 7 is sent to 6, so in total: $2 \mapsto 7 \mapsto 6$,i.e.: $\sigma\tau$ maps 2 to 6. Since we didn't end up where we started, we now want to know where 6 goes, so we start again on the far right, and notice the first time 6 appear is in (15634), meaning 6 goes to 3, and then moving to the left, 3 is next in (2376), so 3 is sent to 7, hence: $6 \mapsto 3 \mapsto 7$, meaning $\sigma\tau$ sends $6to7$. Starting the process for 7, we see it first appears in (27), meaning $7 \mapsto 2$, and then moving left, the next time 2 appears is in (2376), meaning 2 is sent to 3, giving $7 \mapsto 2 \mapsto 3$, so in total $\sigma\tau(7) = 3$. Now beginning with 3, we see the first it appears is in (15634), giving 3 maps to 4; moving left, 4 does not appear any more, so $\sigma\tau(3) = 4$. Starting with 4, we see 4 goes to 1 in (15634), and then 1 goes to 5 in (15), meaning $\sigma\tau(4) = 5$. Then, beginning with 5, we see 5 goes to 6 in (15634), and then 6 goes to 2 in (2376), meaning $\sigma\tau(5) = 2$. But we started at 2, so this is where the cycle ends. So far, then, we have that $\sigma\tau$ contains the cycles (1)(267345). But this contains all of the elements appearing in σ and τ, giving

$$\sigma\tau = (267345)$$

(omitting the 1-cycle (1) which fixes the element 1).

The best way to get used to cycle compositions is to practise... a lot. Here are some answers to products; do try to work through them!

(1) (2456)(123) = (145623)
(2) (3217)(247) = (17)(243)
(3) (63412)(5)(132) = (14)(2)(36) = (14)(36)
(4) (134)(125)(234) = (12453)

(5) (12)(1435)(13) = (152)(34)
(6) (15)(14)(13)(12) = (12345)

4.3. **Properties of Permutations.** Now that we are comfortable with cycle notation, we can start to state some important properties and results.

Theorem 4.1. Products of Disjoint Cycles If X is a finite set, then any permutation of X can be written as a product of disjoint cycles

Proof. Let $\sigma \in S_n$, a permutation of $X = \{1, 2, \ldots, n\}$. We begin by picking any element of X, call it x_1. We then form a sequence by repeatedly applying σ to x_1:

$$x_2 := \sigma(x_1), \qquad x_3 := \sigma(\sigma(x_1)) = \sigma^2(x_1), \qquad x_4 := \sigma^3(x_1),\ \&c$$

This gives us a sequence $(x_1, x_2, x_3, \ldots) = (x_1, \sigma^2(x_1), \sigma^3(x_1), \ldots)$. But σ is a bijective map from X to itself, and X is finite, which means that somewhere along the line, we will repeat two elements: i.e.: for some $j, k \in \mathbb{N}$ with $j < k$, we will have $\sigma^j(x_1) = \sigma^k(x_1)$, which means that if we multiply by σ^{-j}, we have $x_1 = \sigma^{k-j}(x_1)$, where $(k - j) \in \mathbb{N}$. For simplicity, call $m := k - j$, meaning $\sigma^m(x_1) = x_1$. Thus, we can express:

$$\sigma = (x_1 x_2 x_3 \ldots x_m) \cdots$$

The reason we write $\cdots$ after the cycle is because we may have not hit all of the elements of X in that sequence. The way to remedy this is to pick some element of X which does not appear in that cycle, and start the process again. i.e.: call it y_1, and form the sequence $\{y_1, \sigma(y_1), \sigma^2(y_1), \ldots\}$ until you discover the ℓ such that $\sigma^\ell(y_1) = y_1$, giving:

$$\sigma = (x_1 x_2 x_3 \ldots x_m)(y_1 y_2 \ldots y_\ell) \cdots$$

We know that $y_i \neq x_j$ for any $i, j \in \mathbb{N}$, since if they were, this would mean $\sigma^a(x_1) = \sigma^b(y_1)$, giving $\sigma^{b-a}(y_1) = x_1$, putting y_1 in the same cycle as x_1. Thus the two cycles we've deduced are disjoint. We can continue to create new disjoint cycles to represent σ, and since X is finite, this process will terminate, meaning

$$\sigma = (x_1 x_2 x_3 \ldots x_m)(y_1 y_2 \ldots y_\ell) \cdots (z_1 z_2 \ldots z_p)$$

a product of disjoint cycles. □

Writing things in disjoint cycle form has another advantage, namely

Theorem 4.2. If $\alpha, \beta \in S_n$, and they do not share any entries, then $\alpha\beta = \beta\alpha$; i.e.: Disjoint Cycles Commute

Proof. Let $\alpha = (a_1 a_2 \ldots a_k)$, $\beta = (b_1 b_2 \ldots b_m)$, and $a_i \neq b_j$ for any i, j. Let X be the set of size n being permuted by α, β, and let $x \in X$. There are three possibilities: $x = a_i$ some i; $x = b_j$ some j, or x is none of the a_i, b_j.
If $x = a_i$, then it is fixed by β: $\alpha(\beta(x)) = \alpha(\beta(a_i)) = \alpha(a_i)$. Since $\alpha(a_i)$ is some other a_ℓ, this is also fixed by β: $\beta(\alpha(x)) = \beta(\alpha(a_i)) = \alpha(a_i)$. Thus, if $x = a_i$, then $\beta(\alpha(x)) = \alpha(\beta(x))$.
If $x = b_j$, then by the same reasons above, $\beta(\alpha(x)) = \alpha(\beta(x))$, since α fixes any element of β.
If x is any element of X and isn't any of the a_i, b_j, then it does not appear in either α or β, and thus must be fixed by both, i.e.: $\alpha(x) = \beta(x) = x$. So since they both act as the identity, it's clear that $\beta(\alpha(x)) = \alpha(\beta(x))$.
Since these are all the possible cases, we conclude that for any disjoint cycles α, β, we have $\alpha\beta = \beta\alpha$. □

Since the operation in the group S_n is composition of functions, the expression α^k for some $\alpha \in S_n$ means repeated applications of the permutation α. So for $x \in X$, $|X| = n$,

$$\alpha^k(x) = \underbrace{\alpha(\alpha(\alpha(\dots(\alpha(x)))))}_{k-\text{times}}$$

So the *order* of a permutation is the smallest $k \in \mathbb{N}$ such that $\alpha^k = e$, the smallest number of times you have to apply the permutation α to itself to obtain the identity permutation. One of the other advantages to writing permutations in disjoint cycle form is we can immediately figure out the order of the permutation by inspection:

Theorem 4.3. If X is a set of size n, then the order of a permutation $\alpha \in S_n$ written in disjoint cycle form is the least common multiple of the size (or 'length') of the cycles

Proof. If α is a single cycle with m elements in it, then its order is m, which is left as an exercise. Let α be a permutation of length m, and let β be a permutation of length k, and let them be disjoint. let $\ell = \text{lcm}(m, k)$. Then, since disjoint cycles commute, $(\alpha\beta)^\ell = \alpha^\ell\beta^\ell = ee = e$. The reason $\alpha^\ell = e$ is because $\ell = mc$ for some $c \in \mathbb{N}$ (by definition of lowest common multiple), so $\alpha^\ell = (\alpha^m)^c = e^c = e$. The same is true for β^ℓ. Thus, since $(\alpha\beta)^\ell = e$, ℓ must be a multiple of $|\alpha\beta|$. So define $t := |\alpha\beta|$, i.e.: $e = (\alpha\beta)^t = \alpha^t\beta^t$ (and ℓ divides t). If $e = \alpha^t\beta^t$, this means that $\alpha^t = \beta^{-t}$, but since they are disjoint and power of them are necessarily disjoint, the only way they can be inverses is if $\alpha^t = \beta^{-t} = e$. This means that t has to be divisible by both $m = |\alpha|$ and $k = |\beta|$, and so it must also be divisible by the lowest common multiple of k and m. Hence $\ell|t$, and $t|\ell$, so $t = |\alpha\beta| = \text{lcm}(k, m) = \ell$. □

One of the most important kind of permutations is a length 2 cycle, one of the form (ab). These are called *transposition*, as they transpose (switch) a and b. We have the following nice theorem relating any permutation and transpositions:

Theorem 4.4. Product of 2-Cycles For $n > 1$, any $\alpha \in S_n$ is a product of transpositions.

Proof. First, we notice that one of the many ways we can write the identity of S_n is $e = (12)(12)$, so it is a product of 2-cycles (indeed, $e = (ab)(ab)$ for any a, b in the set of n elements). Next, Consider α a single cycle, $\alpha = (a_1a_2 \dots a_k)$. We notice that we can write

$$\alpha = (a_1a_k)(a_1a_{k-1})\cdots(a_1a_3)(a_1a_2) \tag{4}$$

Which is a product of 2-cycles. Now, let α be any permutation. We can write it as a product of disjoint cycles, and then expand each of those in the above method, making it a product of 2-cycles. □

It is important to note: the theorem does not say that we can write any permutation as a product of *disjoint* 2-cycles, just that we can write them as a product of 2-cycles.
Examples

- $(123456) = (16)(15)(14)(13)(12)$
- $(123456) = (561234) = (54)(53)(52)(51)(56)$
- $(145)(6723) = (15)(14)(63)(62)(67)$
- $(13)(4256) = (13)(46)(45)(42)$

Lemma 4.1. If the identity $e \in S_n$ is decomposed as a product of 2-cycles, the decomposition always is an even number of 2-cycles.
The proof is left as an exercise.

Looking at the first two examples, we see that the decomposition into 2-cycles is definitely not unique. There is one aspect about any such decomposition, though, which remains constant:

Theorem 4.5. Let $\alpha \in S_n$, $n > 1$. If α can be decomposed into a product of an even (odd) number of transpositions, then *any* decomposition of α into a product of transpositions will have an even (odd) number of transpositions.

Proof. Let $\alpha = t_1 t_2 \cdots t_r = \tau_1 \tau_2 \cdots \tau_s$, where t_i, τ_j are transpositions. This means that

$$\begin{aligned} e &= t_1 t_2 \cdots t_r \tau_1^{-1} \tau_2^{-1} \cdots \tau_s^{-1} \\ &= t_1 t_2 \cdots t_r \tau_1 \tau_2 \cdots \tau_s \end{aligned}$$

since any transposition is its own inverse (its order is its length, 2). By the previous lemma, since this product of 2-cycles is the identity, its length (r+s) must be even. The only way a sum of two numbers is even is if they're both odd or they're both even. □

Definition 4.1. Let $\sigma \in S_n$ for any n. If you can decompose σ as a product of an even number of transpositions, then σ is called an *even* permutation. If σ can be decomposed as product of an odd number of transpositions, then σ is called an *odd* permutation.

This definition tends to cause some confusion when first learned. For example, the permutation $(123) \in S_3$ is an even cycle, even though it has an odd length. This is because $(123) = (13)(12)$. Don't confuse cycle length with it being an even or an odd permutation!

Theorem 4.6. The set of all even permutations of S_n forms a group. This is called the *Alternating group on n elements*, and is denoted A_n.

Proof. Let $\sigma, \alpha \in S_n$, such that both are even permutations. This means that

$$\begin{aligned} \sigma &= t_1 t_2 \cdots t_{2k} \\ \alpha &= \tau_1 \tau_2 \cdots \tau_{2m} \end{aligned}$$

where the t_i, τ_j are transpositions. Then we see

$$\sigma\tau = t_1 t_2 t_3 \cdots t_{2k} \tau_1 \tau_2 \tau_3 \cdots \tau_{2m}$$

Which is a product of $2k + 2m = 2(k + m)$ transpositions, i.e.: an even number of transpositions. Since we know from Theorem 5.5 that a decomposition is always even or odd, this means that $(\sigma\tau)$ is always an even permutation when σ and τ are even permutations. The identity is always an even permutation, so the set of even permutations is nonempty. So by the finite subgroup test, $A_n := \{\sigma \in S_n \,|\, \sigma \, \text{is an even permutation}\, \}$ is a subgroup of S_n. □

Example: Consider S_4, the permutations on a 4 element set. If we list all of the permutations, we see:

$$\begin{aligned} S_4 = \{&e, (12), (13), (14), (23), (24), (34), (123), (124), (134), (132), (142), (143), \\ &(234), (243), (12)(34), (13)(24), (14)(23), (1234), (1243), (1324), (1342), (1423), (1432)\} \end{aligned}$$

Now we want to take only the even permutations, the ones which can be written as a product of an even number of transpositions. Since we only have 4 elements we're permuting, the even permutations must be of the form $(xy)(zw)$, and $(xyz) = (xz)(xy)$. Hence, we see:

$$A_4 = \{e, (123), (124), (134), (132), (142), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$$

If we count the elements, we see that A_4 has exactly half the number of elements as S_4. It turns out this is always true:

Theorem 4.7. Let $n > 1$. Then $|S_n| = n!$, and $|A_n| = n!/2$.

Proof. The permutations of S_n permute the set of n elements. Number them $\{1, 2, \dots, n\}$ as usual. First, we must choose where 1 is sent, for which there are n choices. Once chosen, we choose where 2 is sent, and now we have $n-1$ choices, since we've already chosen where 1 goes. Then we choose where 3 goes, and we have $n-2$ choices, until we get to n, and there is only 1 choice, meaning in total, there are $n(n-1)(n-2)\cdots 2\cdot 1 = n!$ choices for permutations.
If σ is an odd permutation, then $(12)\sigma$ is even, and $(12)\sigma = (12)\alpha$ if and only if $\sigma = \alpha$ (because we can use the cancellation law). Hence, we have at least as many odd as even permutations. But similarly, for every even permutation β, $(12)\beta$ is an odd permutation, and $(12)\beta = (12)\gamma$ if and only if $\beta = \gamma$. So there are at least as many even as odd permutations. Hence, there must be an equal number of both, meaning $|A_n| = n!/2$. □

Our go-to group, $\mathrm{GL}(n, \mathbb{R})$ can also be thought of as a kind of permutation group, but the set of elements it's acting on is a particular vector space. Permutations are bijections from a set to itself, which the elements of $\mathrm{GL}(n, \mathbb{R})$ certainly are, but additionally they preserve the structure of the vector space. We will see more of this sort of mapping in the section on homomorphisms.

5. Cosets, Normal Subgroups, Lagrange's Theorem

We start this section with the notion of *cosets*, which lead directly into normal subgroups, and Lagrange's theorem: the latter is one of the most important theorems about finite groups, and the former helps us form new groups out of groups we already have.

Definition 5.1. Let G be a group, and let $H \subseteq G$. For any $g \in G$, we define the set

$$gH = \{\, gh \,|\, \forall h \in H\}$$

and call gH the *left coset* of H in G containing g. The element g is called the *coset representative* of gH. Similarly, we define

$$Hg = \{\, hg \,|\, \forall h \in H\}$$

to be the *right coset* of H in G containing g. As with all sets, we use $|gH|$ and $|Hg|$ to denote the cardinality of the cosets.

As a note, if the group G we are looking at has addition as its group operation, then we usually write $g + H$ instead of gH for a coset. Now, let's look at some examples
Examples

(1) Let $G = D_3$, and let $H = \{e, r, s, sr^2\}$. Then all of the left cosets of H in G are

$$\begin{aligned} eH &= H \\ rH &= \{r, r^2, rs, rsr^2\} = \{r, r^2, sr^2, sr\} \\ r^2H &= \{r^2, e, r^2s, r^2sr^2\} = \{r^2, e, sr, s\} = sH \\ (sr)H &= \{sr, sr^2, srs, r\} = \{sr, sr^2, r^2, r\} \\ (sr^2)H &= \{sr^2, s, sr^2s, e\} = \{sr^2, s, r, e\} \end{aligned}$$

(2) Let $G = \mathbb{Z}_6$,and let $H = \{0, 2, 4\}$. Then the left cosets are

$$\begin{aligned} 0 + H &= \{0, 2, 4\} = 2 + H = 4 + H = H \\ 1 + H &= \{1, 3, 5\} = 3 + H = 5 + H \end{aligned}$$

(3) Let $G = S_3$, and let $H = \{e, (123)\}$. The right cosets are

$$\begin{aligned} He &= H \\ H(12) &= \{(12), (123)(12)\} = \{(12), (13)\} \\ H(13) &= \{(13), (123)(13)\} = \{(13), (23)\} \\ H(23) &= \{(23), (123)(23)\} = \{(23), (12)\} \\ H(123) &= \{(123), (123)(123)\} = \{(123), (132)\} \\ H(132) &= \{(132), (123)(132)\} = \{(132), e\} \end{aligned}$$

We notice a couple of things from our examples. Firstly, we notice that cosets usually are not usually subgroups; for example, $H(12) = \{(12), (13)\} \subset S_3$ is not a subgroup. Secondly, we see that gH is not always equal to Hg; still from the S_3 example, we see $H(13) = \{(13), (23)\}$, but $(13)H = \{(13), (12)\} \neq H(13)$. Lastly, we see that the same coset may have different representatives: in the first example, $r^2H = sH$, even though $r^2 \neq s$.
When the subset $H \subseteq G$ is a subgroup, many nice things happen. We will show the properties for left cosets, but analgous results hold for right cosets.

Lemma 5.1. Properties of Cosets of Subgroups Let G be a group, and $H \leqslant G$ a subgroup. Let $x, y \in G$. Then

(1) $x \in xH$
(2) $xH = H$ if and only if $x \in H$
(3) $xH = yH$ if and only if $y^{-1}x \in H$
(4) $xH = yH$ or $xH \cap yH = \varnothing$
(5) $|xH| = |yH|$
(6) $xH = Hx$ if and only if $xHx^{-1} = H$
(7) The only coset which is also a subgroup is H itself.

Proof. (1) Since H is a subgroup, this means $e \in H$, so for any $x \in G$, $xe = x \in xH$.
(2) i) $\Rightarrow$ if $xH = H$, then $xe = x \in xH$.
$\Leftarrow$ We proceed by showing double containment. First, if $x \in H$, then $xH \subseteq H$ since H is closed under its operation. Second, let $h \in H$ be any element. Since $x \in H$, this means $x^{-1}h \in H$, and hence $h = eh = (xx^{-1})h = x(x^{-1}h) \in xH$, meaning $H \subseteq xH$, and thus $H = xH$ when $x \in H$.
(3) $xH = yH$ if and only if $y^{-1}xH = H$, so using the previous property, the result follows
(4) First, assume $xH \cap yH \neq \varnothing$, and let $a \in xH \cap yH$. This means $\exists h_1, h_2 \in H$ with $xh_1 = a = yh_2$. Hence $x = ah_1^{-1} = yh_2h_1^{-1}$, meaning $xH = yh_2h_1^{-1}H = yH$, by property (2).
(5) Consider the map $f : xH \to yH$, mapping $xh \mapsto yh$ for every $h \in H$. This map is injective (1-1) since if $yh_1 = yh_2$, then $h_1 = h_2$ by the cancellation law, and hence for finite groups, this is sufficient to show that $|xH| = |yH|$. (How would we have to adapt this for infinite groups?)
(6) If $xH = Hx$, then right multiplying by x^{-1} gives $xHx^{-1} = H$. Similarly, starting with $xHx^{-1} = H$ and right multiplying by x gives $xH = Hx$
(7) If xH is a subgroup, it must contain e, the identity. Using previous properties, we know $xH \cap eH \neq \varnothing$ if xH is a subgroup, but this must mean $xH = eH = H$. Conversely, $x \in H$ implies $xH = H$. □

As Gallian rightfully points out, it's useful to rephrase these properties in terms of words, to get a good idea of what they say. Number 1 says the "left coset containing x" really does contain x. The property that $hH = H$ for any $h \in H$ colloquially says that H "absorbs" (or indeed, "eats") elements of itself. The third property allows to relate questions about a coset (of H) and H itself,

and property 6 allows us to do a similar exchange. The last property tells us that only one coset of H is a subgroup (instead of just a subset), and that is H itself.
Properties 4 and 5 together are very important: they tell us that for a given H, all left (or right) cosets are the same size, and any two cosets are equal or disjoint. This means that any given coset is entirely determined by any element, so you just need one representative of a coset to determine the whole coset. The disjoint property means that for a group G, and a subset H, the left (or right) cosets of H effectively sub-divide the group into a collection of disjoint, equal-sized subsets. In fact, the cosets of H induce an *equivalence relation* on G: you could say for $x, y \in G$, $x \sim_H y$ if and only if $xH = yH$. As an exercise, prove that this is actually an equivalence relation.

5.1. **Lagrange's Theorem.** We now will introduce one of the most important theorems in finite group theory, and indeed, this course:

Theorem 5.1. Lagrange's Theorem Let G be a finite group, and H a subgroup of G. Then $|H|$ divides $|G|$. Furthermore, the number of distinct left (or right) cosets of H in G is the value $|G|/|H|$.

Proof. We'll proceed using left cosets; the proof is nearly identical for right cosets. Let $g_1H, g_2H, \ldots, g_kH$ be all of the left cosets of H in G which are distinct. What this means is that for any $g \in G$, gH must be equal to g_iH for some i. By the preceding lemma, we know that for any $g \in G$, $g \in gH$, meaning that each of the elements of G is contained in one coset. Hence, we see

$$G = \bigcup_{i=1}^{k} g_iH = g_1H \cup g_2H \cup \ldots \cup g_kH$$

The lemma also stated that the cosets are disjoint, and that each coset is of the same size, so we can conclude that

$$\begin{aligned} |G| &= |g_1H| + |g_2H| + \ldots + |g_kH| \\ &= k|H| \end{aligned}$$

Meaning that $|H|$ divides $|G|$, and since k is the number of distinct cosets, we have $k = |G|/|H|$. □

Incredibly Important Remark: The converse of Lagrange's theorem is powerfully false. The theorem says that the order of a subgroup divides the order of a group. It is very much *not* true, however, that given a group of order n, there necessarily exists subgroups of order each of the divisors of n. For example, $|A_4| = 12$, but there is no subgroup of order 6, even though $6|12$.
There are many important corollaries to Lagrange's theorem. First, we introduce a useful notation

Definition 5.2. Let G be a finite group, and let H be a subgroup. The number of left (right) cosets of H in G is called the *index of H in G*, and is denoted $|G : H|$.

Corollary 5.1. If G is a finite group, and $H \leqslant G$, then $|G : H| = |G|/|H|$.

Corollary 5.2. Let G be a finite group, $g \in G$. Then $|g|$ divides $|G|$.

Proof. $|g| = |\langle g \rangle|$, $\langle g \rangle \leqslant G$. □

Corollary 5.3. A finite group of prime order must be cyclic.

Proof. If $|G| = p$, a prime, then for any $g \in G$, $|g|$ divides $|G|$. But for any $g \neq e$, this means $|g| \neq 1$, so we must have $|g| = p$. □

Corollary 5.4. Let G be a finite group, $g \in G$. Then $g^{|G|} = e$.

Proof. We know $|g|$ divides $|G|$. This means $|G| = x|g|$ for some $x \in \mathbb{N}$. Hence

$$g^{|G|} = g^{x|g|} = (g^{|g|})^x = e^x = e$$

□

Theorem 5.2. Cauchy's Theorem Let G be a finite group, and let p be a prime dividing $|G|$. Then G has an element of order p.

Proof. The proof is omitted, as the tools needed for a complete proof are a little advanced for the course. □

5.2. **Normal Subgroups.** Now that we've built up a fair amount of knowledge regarding cosets, we can define a very significant class of subgroups. We've seen that for a given subgroup $H \leqslant G$, the left and right cosets are not always equal, i.e.: for every $g \in G$, it's not always true that $gH = Hg$. For certain subgroups, this is true, and they turn out to be of critical importance

Definition 5.3. Normal Subgroups Given a group G, a subgroup $H \leqslant G$ is called *normal* if $gH = Hg$ for all $g \in G$. Equivalently, if $gHg^{-1} = H$ for all $g \in G$. We denote such a normal subgroup by $H \trianglelefteq G$.

Important Remark: The definition of normal tends to give students trouble at first. We remember that gH is a set of elements, $gH = \{gh_1, gh_2, gh_3, \ldots\}$ over all elements $h_i \in H$, and similarly for Hg. So saying that $gH = Hg$ means that these are equivalent as *sets*:

$$\{gh_1, gh_2, gh_3, \ldots\} = \{h_1g, h_2g, h_3g, \ldots\}$$

But remember that the order in which we writes elements in a set doesn't matter. So the equality between the sets just means that each element in the left set is equal to some element of the right set. In other words, if $gH = Hg$, then for any $h \in H$, there exists and $h' \in H$ with $gh = h'g$. The important thing here is that h and h' do not have to be equal (many students see $gH = Hg$ and presume this means $gh = hg$, which is usually false)

Theorem 5.3. Normal Subgroup Test A subgroup $H \leqslant G$ is normal if and only if $gHg^{-1} \subseteq H$ for all $g \in G$.

Proof. We know that the definition of a normal subgroup is one such that $gHg^{-1} = H$ for all $g \in G$, i.e.: for any $h \in H$, and $g \in G$, there exists an $h' \in H$ such that $ghg^{-1} = h'$. Hence $H \trianglelefteq G$ implies $gHg^{-1} \subseteq H$ for all $g \in G$.
Now, suppose $gHg^{-1} \subseteq H$ for all $g \in G$. If we multiply appropriately, we get $H \subseteq g^{-1}Hg$ for <u>all</u> $g \in G$. Hence, $gHg^{-1} = H$, meaning it's normal. □

Examples

(1) Let G be an abelian group. Then every subgroup H is normal in G, since in this particular case $gh = hg$ for every $g \in G, h \in H$.
(2) For any group G, the centre $Z(G)$ is normal in G for the same reason as in example 1.
(3) A_n is a normal subgroup of S_n. (You can justify this with cycle types, and the sorts of products you get in σA_n, $A_n\sigma$ for $\sigma \in S_n$)
(4) Let $G = D_n$, then the subgroup of rotations $\langle r \rangle =: R \leqslant D_n$ is a normal subgroup. We know that for any rotation r^k, and any reflection x, we have $r^kx = xr^{-k}$. And since the rotations commute, we can conclude that $gR = Rg$ for all $g \in D_n$.
(5) For any group G, the subgroups G and $\{e\}$ are both trivially normal in G.

Most subgroups need to be tested to see if they are normal, but there is a special class of subgroups of finite groups which are always normal

Theorem 5.4. Let G be a finite group, and let H be a subgroup of G of index 2, i.e.: $|G:H| = 2$. Then H is normal in G.

Proof. Since $2 = |G:H| = |G|/|H|$, we know from the corollaries to Lagrange's Theorem that the number of cosets of H in G is 2. Let $g \in G$ such that $g \notin H$, then the two cosets we have are H and gH. Since we know that the cosets partition G, we must have $gH = G \setminus H = \{g \in G \mid g \notin H\}$. Similarly, the two right cosets are H, Hg for that $g \in G \setminus H$ we chose above. Again, since the cosets partition, we must have that $G \setminus H = Hg$, and hence we have $gH = Hg$, i.e.: every left coset is also a right coset. Since it didn't matter what element $g \in G \setminus H$ we chose, we conclude that H is normal. □

From this theorem, we can immediately see that A_n must be normal in S_n, and that the rotations must be normal in D_n.

Definition 5.4. Let G be any group, and let $H \subseteq G$. We define the *normaliser* of H in G to be

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

As a direct result of this, we see

Proposition 5.1. Let G be a group, and let H be a subgroup. H is normal in G if an only if $N_G(H) = G$.

The proof of this is direct and just involves unwinding definitions, and so is left as an exercise. One of the main reasons that normal subgroups are so important is that they allow us to take groups and form new groups by "reducing" them. We will see this soon when we get to quotient groups.

6. Homomorphisms, Isomorphisms, Automorphisms

6.1. **Homomorphisms.**

Back in our linear algebra days, we saw that $\mathrm{GL}(n, \mathbb{R})$ was the set of invertible linear transformations from an n-dimensional real vector space to itself. We also looked at linear transformations from vector spaces to other vector spaces. These were maps of sets which also preserved the structure of the object we were looking at.

We want to look at similar maps, in the context of groups: maps between the sets that comprise the groups, which also preserve the group structures of both. In this way, we can determine which groups "look the same", in that they would be the same size and have the same group structure.

Definition 6.1. Homomorphism Let $(G, \cdot)$, $(H, *)$ be groups. A *group homomorphism* from G to H is a map $\varphi : G \to H$ such that for all $g_1, g_2 \in G$, we have

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) * \varphi(g_2)$$

When we do not specify what the group operations are, we will follow the previous notation and say

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$$

but we must remember the products live in different places: the product on the left occurs in G, and then we map the elements; on the right hand side, we map each to H, and then the product occurs in H.

For any group homomorphism, there is a subgroup of the domain which is very important

Definition 6.2. Kernel Let G, H be groups, and let $\varphi : G \to H$ be a group homomorphism. The *kernel* of φ is the set $\ker \varphi = \{g \in G \mid \varphi(g) = e_H\}$, all of the elements of G which are sent by φ to the identity element of H.

One can draw the parallel to linear transformations: we similarly defined null(A) to be the set of all vectors sent to 0 (the additive identity) by the linear transformation represented by the matrix A.
Since this tends to be an issue for some students at first, let us also define

Definition 6.3. Image Let G, H be groups, and let $\varphi : G \to H$ be a group homomorphism. The *image* of φ is the set $\text{Im}\varphi = \{\varphi(g), \mid \forall\, g \in G\} \subseteq H$. In other words, the image is all of the elements of H which G is sent to.

Before we get into the many properties of homomorphisms, let us look at some examples
Examples

(1) Consider the mapping from $\mathbb{Z}$ to $\mathbb{Z}$ given by $x \mapsto 2x$. This is well defined, and is a group homomorphism as
$$\varphi(x+y) = 2(x+y) = 2x + 2y = \varphi(x) + \varphi(y)$$
and the kernel is just $\{0\}$, since $\varphi(x) = 2x = 0$ implies $x = 0$. The image is $\{2x \mid x \in \mathbb{Z}\}$, all of the even integers.
(2) Let $\varphi : \mathbb{R}^* \to \mathbb{R}^*$, given by $\varphi(x) = x^2$. This is well defined, and is a group homomorphism as $\varphi(xy) = (xy)^2 = x^2y^2 = \varphi(x)\varphi(y)$. In this case, the identity is 1, so $\ker\varphi = \{x \in \mathbb{R}^* \mid x^2 = 1\}$, thus the kernel is the set $\ker\varphi = \{1, -1\}$.
(3) Let G be any group. We can define the *identity homomorphism* $\varphi_{\text{id}} : G \to G$, defined simply as $\varphi_{\text{id}}(g) = g$ for all $g \in G$. It is easy to check this is a homomorphism.
(4) Let G, H be any groups. We can define the *trivial homomorphism* $\varphi : G \to H$ as $\varphi(g) = e_H$ for all $g \in G$. In this case, the kernel is all of G, and the image is just e_H. It is again easy to check this is a homomorphism.
(5) Consider $(\text{Mat}_{n\times n}(\mathbb{R}), +)$, the $n \times n$ real matrices as a group under addition. Then the map $\text{Tr} : \text{Mat}_{n\times n}(\mathbb{R}) \to \mathbb{R}$ is a group homomorphism, since we know $\text{Tr}(A+B) = \text{Tr}(A) + \text{Tr}(B)$.
(6) Consider the map from $\text{GL}(n, \mathbb{R}) \to \mathbb{R}^*$ given by $A \mapsto \det(A)$. This is a group homomorphism, with $\ker\det = \{A \in \text{GL}(n, \mathbb{R}) \mid \det(A) = 1\}$, which we call $\text{SL}(n, \mathbb{R})$.
(7) Let $(G = \{f : \mathbb{R} \to \mathbb{R} \mid \text{bounded, continuous}\}, +)$, and $H = \mathbb{R}$. Fix an element $a \in \mathbb{R}$. Then the map $\varphi : G \to H$, $f \mapsto \lim_{x\to a} f$. This is a group homomorphism.
(8) Consider the map $\varphi : D_3 \to D_6$ defined as follows: $\varphi(r^k) = r^{2k}$, $\varphi(s) = s$, $\varphi(sr^k) = sr^{2k}$. This is a group homomorphism, and is injective since $ker\varphi = \{e\}$.

When constructing homomorphisms, it is important to check whether the map actually defines a function, i.e.: that it is well-defined. What this generally means is that if you have a homomorphism $\varphi : G \to H$, you need to check that $\forall g \in G$, the image $\varphi(g)$ only has one, unambiguous value. For example, one might be tempted to make a homomorphism from $f : \mathbb{Z}_6 \to Z_4$, sending $x \mapsto x \mod 4$. In this case, $f(4) = 0$, meaning $f(4) + f(4) = 0$, but if this were a homomorphism, then $f(4+4) = f(8) = f(2 \mod 6) = 2$. Meaning $2 \mod 6$ would be sent to both 0 and $2 \mod 4$, and hence this is not well defined (and so other properties fail).
Notation: One thing that tends to confuse students is the notation for preimages of maps; this mainly comes from the fact that we use the same notation for preimages and inverses (for a good reason). Let $\varphi : G \to K$ be a map. We do not know if φ is invertible; even if it isn't, we can define the preimage of any point $k \in K$ as follows:
$$\varphi^{-1}(k) = \{g \in G \mid \varphi(g) = k\}$$
In words, the preimage of the element k is the set of *all* the g in G which φ sends to k. If the map φ is invertible, this means that the preimage has only one element in it. If you see φ^{-1}, don't presume that is an 'inverse', unless you know (or can prove) that whatever map φ you have is actually invertible.

6.2. **Properties of Homomorphisms.** There are many useful properties of homomorphisms. We will list them in two separate theorems, one for elements, and one for subgroups:

Theorem 6.1. Elements under Homomorphisms Let G, K be groups, and let $\varphi : G \to K$ be a group homomorphism. For any $g \in G$, we have

(1) $\varphi(e_G) = e_K$
(2) $\varphi(g^n) = \varphi(g)^n$, for all $n \in \mathbb{Z}$
(3) If $|g| < \infty$, then $|\varphi(g)|$ divides $|g|$
(4) $\ker\varphi \leqslant G$
(5) $\varphi(g_1) = \varphi(g_2)$ if and only if $g_1 \ker\varphi = g_2 \ker\varphi$
(6) If $\varphi(g_1) = k$, then $\varphi^{-1}(k) := \{g \in G \,|\, \varphi(g) = k\} = g_1 \ker\varphi$

Proof. (1) $\varphi(g) = \varphi(ge_G) = \varphi(g)\varphi(e_G)$, so using the cancellation law, we get $e_K = \varphi(e_G)$.
(2) $\varphi(g^n) = \varphi(gg\cdots g) = \varphi(g)\varphi(g)\cdots\varphi(g) = \varphi(g)^n$
(3) Let $n = |g|$, so $g^n = e$. Then $e_K = \varphi(e_G) = \varphi(g^n) = \varphi(g)^n$, so from our work on orders, we have that $|\varphi(g)|$ divides $n = |g|$.
(4) Let $g_1, g_2 \in \ker\varphi$. Then $\varphi(g_1) = \varphi(g_2) = e_K$. Let us apply the one step subgroup test. Consider

$$\varphi(g_1g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = e_K\varphi(g_2)^{-1} = e_Ke_K = e_K$$

thus, $g_1g_2^{-1} \in \ker\varphi$. Since $e_G \in \ker\varphi$ always, it's nonempty, and thus is a subgroup by the one step subgroup test.
(5)&(6) left as exercises □

Theorem 6.2. Subgroups under Homomorphisms Let G, K be groups, $H \leqslant G$, and $\varphi : G \to K$ a group homomorphism.

(1) The image of H under φ, $\varphi(H) = \{\varphi(h) \,|\, h \in H\}$ is a subgroup of K.
(2) H cyclic implies $\varphi(H)$ cyclic
(3) H abelian implies $\varphi(H)$ abelian
(4) H normal in G implies $\varphi(H)$ normal in $\varphi(G)$
(5) $|\ker\varphi| = n$ implies φ is an n-to-1 mapping.
(6) $|H| = n$ implies $|\varphi(H)|$ divides n
(7) If J is a subgroup of K, then the preimage $\varphi^{-1}(J) = \{g \in G \,|\, \varphi(g) \in J\}$ is a subgroup of G.
(8) If $J \trianglelefteq K$, then $\varphi^{-1}(J) \trianglelefteq G$.

Proof. (1) Let $\varphi(h_1), \varphi(h_2) \in \varphi(H)$. Then

$$\varphi(h_1)\varphi(h_2)^{-1} = \varphi(h_1h_2^{-1})$$

And since H is a subgroup, $h_1h_2^{-1} \in H$, thus $\varphi(h_1h_2^{-1}) \in \varphi(H)$. It's clearly nonempty, and so is a subgroup.
(2) left as exercise
(3) If H abelian, $h_1h_2 = h_2h_1$ for all $h_i \in H$. Then

$$\varphi(h_1)\varphi(h_2) = \varphi(h_1h_2) = \varphi(h_2h_1) = \varphi(h_2)\varphi(h_1)$$

Thus, $\varphi(H)$ is abelian.
(4) For $\varphi(h) \in \varphi(H), \varphi(g) \in \varphi(G)$, we see

$$\varphi(g)^{-1}\varphi(h)\varphi(g) = \varphi(g^{-1}hg)$$

and since H normal, this means $g^{-1}hg \in H$ for any $g \in G, h \in H$, meaning that $\varphi(g)^{-1}\varphi(h)\varphi(g) \in \varphi(H)$. Thus $\varphi(H) \trianglelefteq \varphi(G)$
(5) Follows from property 6 of the previous theorem, and the fact that we know the cosets of $\ker\varphi$ have the same number of elements (realising that $\ker\varphi = \varphi^{-1}(e)$ by definition)

(6) Let $\varphi_H := \varphi|_H$, the restriction of φ to the elements of H. Thus, $\varphi_H : H \to \varphi(H)$. Let $|\ker \varphi_H| = n$. Then from the previous property, φ_H is an n-to-1 mapping, meaning $n|\varphi(H)| = |H|$.
(7) First, clearly $e_G \in \varphi^{-1}(J)$. Let $g_1, g_2 \in \varphi^{-1}(J)$. Then $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} \in J$, since J is a subgroup. Thus, $g_1 g_2^{-1} \in \varphi^{-1}(J)$, meaning its a subgroup by the one-step subgroup test.
(8) Left as exercise. □

There is a very important corollary to this theorem

Corollary 6.1. Let $\varphi : G \to K$ be an homomorphism of groups. Then $\ker \varphi$ is a normal subgroup of G

Proof. Using property 8 of Theorem 7.2, with $J = \{e_K\}$ (which is always normal). □

We will soon learn the reverse of this is also true: every normal subgroup of G is the kernel of some homomorphism of G. There is another important fact about kernels which is good to remember

Proposition 6.1. Let $\varphi : G \to K$ be a group homomorphism. Then φ is injective (1-1) if and only if $\ker \varphi = \{e_G\}$.

Proof. First, suppose φ is injective. We know that for any homomorphism, $\varphi(e_G) = e_K$. Suppose $g \in G$ is in the kernel: then $\varphi(g) = e_K$, so $\varphi(g) = \varphi(e_G)$. But since φ is 1-1, this means $g = e_G$, so $\ker \varphi = \{e_G\}$.
Second suppose $\ker \varphi = \{e_G\}$. Let $g, h \in G$ such that $\varphi(g) = \varphi(h)$. These are group elements in K, so we can multiply by inverses. Using all the knowledge we have of homomorphisms so far, we see

$$\begin{aligned}\varphi(g) = \varphi(h) \;\Rightarrow\; e_K &= \varphi(h)\varphi(g)^{-1} \\ &= \varphi(h)\varphi(g^{-1}) \\ &= \varphi(hg^{-1})\end{aligned}$$

Meaning $hg^{-1} \in \ker \varphi$. But the only thing in the kernel is the identity, so $hg^{-1} = e_G$, meaning $h = g$. So $\varphi(g) = \varphi(h)$ gives us $g = h$, meaning φ is 1-1. □

As a note if we have a map $f : X \to Y$ which is injective, we sometimes write $f : X \hookrightarrow Y$. Another important and useful fact to keep in mind is the following

Proposition 6.2. Let S, T be finite sets of the same size, $|S| = |T|$. Let $f : S \to T$ be a map. Then f injective implies f bijective. Similarly, f surjective implies f bijective.

Proof. This is relatively straightforward, and is a good exercise to try to prove □

6.3. **Isomorphisms.**

Definition 6.4. Let G, K be groups, and let $\varphi : G \to K$ be a group homomorphism. If φ is bijective (i.e.: 1-1 and onto), then we say that φ is an *isomorphism.* If there exists an isomorphism between G and K, we say the two groups are *isomorphic*, and denote it by $G \cong K$.

Isomorphisms are very special kinds of maps. If two groups are isomorphic, this means that they have the same size, and the same group structure (since homomorphisms respect group operations). In essence, two groups which are isomorphic are "the same": you can identify the elements and group operation of one exactly with those of the other. It is important to note, though, that "isomorphic" is different from "equal". For example, the additive groups

$$G = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}; \qquad H = \left\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Q}\right\}$$

are isomorphic, but they are not equal. The elements of G are real numbers, and the elements of H are 2×2 matrices, which cannot be equal. Saying the groups are isomorphic, however, means we can bijectively identify the elements of G and H in a way that the group operations are the same. Hence, $G \cong H$, but $G \neq H$. This is a somewhat pedantic point, I agree, since "isomorphic" means "for all intents and purposes, the same", and "equals" means "precisely the same", which are pretty close.
Examples

(1) Clearly, any group G is isomorphic to itself, under the identity homomorphism.
(2) Let $G = \mathbb{Z}_2$, and let $H = \{1, -1\}$ under multiplication. To emphasise that G is a set of equivalence classes (i.e.: $x \sim y$ if and only if $x - y = 2m$ some $m \in \mathbb{Z}$), write $G = \{\bar{0}, \bar{1}\}$. Then the map $\varphi : G \to H$ given by $\varphi(\bar{0}) = 1$, $\varphi(\bar{1}) = (-1)$ is an isomorphism.
(3) Let $G = 2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6 \ldots\}$, $H = 3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$. Then $G \cong H$ via the map $\varphi(2x) = 3x$. It isn't hard to check that this is well defined (the image is a single, unambiguous number). The kernel is just $\{0\}$, since $\varphi(2x) = 3x = 0$ implies $x = 0$, meaning $2x = 0$. It's clearly surjective, and $\varphi(2x + 2y) = \varphi(2(x + y)) = 3(x + y) = 3x + 3y = \varphi(2x) + \varphi(2y)$.
(4) Expanding on the previous example, $m\mathbb{Z} \cong n\mathbb{Z}$ for any $n, m \in \mathbb{Z} \setminus \{0\}$.
(5) Let $G = S^1 = \{e^{i\theta} \mid \theta \in [0, 2\pi)\}$ under complex multiplication. This is the circle, the set of length 1 complex numbers. Let $K = [0, 1)$ the real unit interval under addition modulo 1. i.e.: if $x, y \in [0, 1)$, then $x + y \equiv (x + y) \mod 1$ (it's not hard to check that this is a group) Then $G \cong K$ via the morphism $e^{i\theta} \mapsto (\theta/2\pi) \mod 1$. This can be seen via:

$$\varphi(e^{i\theta_1}e^{i\theta_2}) = \varphi(e^{i(\theta_1+\theta_2)}) = (\theta_1 + \theta_2)/2\pi = \theta_1/2\pi + \theta_2/2\pi = \varphi(e^{i\theta_1}) + \varphi(e^{i\theta_2})$$

The kernel is just $e_G = 1$, since if $\varphi(e^{i\theta}) = 0$, then $\theta/2\pi \equiv 0 \mod 1$, meaning θ is an integer multiple of 2π, which isn't in the domain unless the multiple is 0. It is surjective because if $y \in [0, 1)$, then the element $e^{i(2\pi y)}$ is sent to y.

As with homomorphisms, we have a list of properties of isomorphisms acting on group elements, and on subgroups. Many of them are the same, so we'll only list the major differences

Theorem 6.3. Isomorphisms acting on Elements Let $\varphi : G \to K$ be an isomorphism of groups. Then

(1) $|g| = |\varphi(g)|$ for all $g \in G$
(2) $G = \langle g \rangle$ if and only if $K = \langle \varphi(g) \rangle$

Proof. Considering our knowledge of homomorphisms, and using the added knowledge that the map we're given is a bijection, these two properties are left as an exercise. □

Number (2) above is important; it says that given an isomorphism of cyclic groups, generators of the first are sent to generators of the second.

Theorem 6.4. Isomorphisms acting on Subgroups Let $\varphi : G \to K$ be an isomorphism of groups. Then

(1) The map $\varphi^{-1} : K \to G$, which takes an element to its preimages, is an isomorphism.
(2) G cyclic if and only if K cyclic

Proof. (1)(Outline) Since φ is bijective, this means that for any element in $k \in K$, the preimage $\varphi^{-1}(k)$ has only one element, and so $\varphi^{-1} : K \to G$ is a well defined map. Now, it is required to show it's bijective, and respects group operation.
(2) Related to the previous theorem, left as an exercise □

We can now offer an alternate definition of a subgroup of a group. Given a group homomorphism $\varphi : G \to K$ which is injective but not surjective, G and K are not isomorphic, but it is easy to show that it's always true that G is isomorphic to $\varphi(G)$, the image of G under φ (do this as an exercise).

Definition 6.5. Let G be a group. A *subgroup* of G is a group H, together with an injective group homomorphism $\varphi : H \hookrightarrow G$.

It is left as an exercise to show that this is equivalent to the definition given before.

6.4. **Automorphisms.** When we looked at basic examples of isomorphisms, we noted that the identity map was an isomorphism from a group G to itself. Now it might be reasonable to ask if that is the only isomorphism of G to itself, or if there are more. We can easily cook up some examples:

1. Let $G = (\mathbb{R}, +)$, and consider the map $\varphi : \mathbb{R} \to \mathbb{R}$, $x \mapsto -x$. This is an isomorphism.
2. Let $G = \mathbb{R}^2$ under pointwise addition: $(a, b) + (c, d) = (a + c, b + d)$. Then the map $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$, $(a, b) \mapsto (b, a)$ is an isomorphism.
3. Let $G = \mathbb{C}$ under addition. The map from G to itself defined by $z \mapsto \bar{z}$, sending a complex number to its conjugate, is an isomorphism from $\mathbb{C}$ to itself.
4. Let $G = \mathbb{R}^n$, a group under addition. Let $A \in \mathrm{GL}(n, \mathbb{R})$. Then A defined an invertible linear transformation from $\mathbb{R}^n$ to itself, which is (practically by definition) an isomorphism.
5. Let G be any group. The map $G \to G$, sending $g \mapsto g^{-1}$ is an isomorphism if and only if G is abelian.

So, since there are non-identity isomorphisms from the group to itself, we can define

Definition 6.6. Let G be a group. An isomorphism $\varphi : G \to G$ is called an *automorphism* of G. We denote the set of all automorphisms of G by $\mathrm{Aut}(G)$.

There is a particular type of automorphism that turns out to be very important. We start with a definition.

Definition 6.7. Let G be a group, and fix an $h \in G$. Then taking any $g \in G$, the map $g \mapsto h^{-1}gh$ is called *conjugation by h.* If we denote this map $\varphi_h : G \to G$ (for our fixed h), the φ_h is an automorphism of G called an *inner automorphism.* We denote all of the inner automorphisms of G by $\mathrm{Inn}(G)$.

The reason $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are important to consider is because of the following very-nice-theorem:

Theorem 6.5. Let G be any group. Then $\mathrm{Aut}(G)$ is a group under function composition, and $\mathrm{Inn}(G)$ is a subgroup of it.

Proof. All of the elements of $\mathrm{Aut}(G)$ are bijections from a set (G) to itself, which respect the group operation. We've already proven that *all* of the bijections from a set to itself form a group under composition, so since $\mathrm{Aut}(G)$ is contained in the set of all bijections, we just need to show $\mathrm{Aut}(G)$ is a subgroup. Let φ, ψ be automorphisms of G. We need to show that $\varphi \circ \psi$ is an automorphism (we already know that φ^{-1} is an automorphism via Theorem 7.4). Let $g, h \in G$, and define $f := \varphi \circ \psi$. Then

$$f(gh) = \varphi \circ \psi(gh) = \varphi(\psi(gh)) = \varphi(\psi(g)\psi(h)) = \varphi(\psi(g))\varphi(\psi(h)) = f(g)f(h)$$

So $\varphi \circ \psi \in \mathrm{Aut}(G)$. Hence, $\mathrm{Aut}(G)$ is a subgroup of all of the bijections of G (meaning $\mathrm{Aut}(G)$ is a group itself).
Showing $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$ is left as an exercise. □

Determining $\text{Aut}(G)$ is not always easy, nor straightforward. On the other hand, determining $\text{Inn}(G)$ just involves listing φ_g for all $g \in G$, and then figuring out which ones give you the same map (since you could have $\varphi_g = \varphi_h$ even if $g \neq h$).

Examples

(1) Let G be an abelian group. Then $\text{Inn}(G)\cong \{e\}$. This is because for any $h \in G$, $\varphi_h(g) = h^{-1}gh = h^{-1}hg = eg = g = \text{id}(g)$ for any $g \in G$. Hence, all inner automorphisms act as the identity automorphism.

(2) Let $G = \mathbb{Z}_{10}$. This means that $G = \langle 1\rangle$. But, we know all of the other elements which generate the groups, from our section on cyclic groups. $G = \langle 1\rangle = \langle 3\rangle = \langle 7\rangle = \langle 9\rangle$. We know from theorem 7.4 that an isomorphism between cyclic groups must send generators to generators. We also can determine that the morphism is entirely determined by where we send the generator 1: $\varphi(n) = \varphi(n \cdot 1) = \sum_{k=1}^{n} \varphi(1)$. So the only places we can send 1 are 1,3,7,9. So if we call φ_n the map taking 1 to n, then $\text{Aut}(G) = \{\varphi_1, \varphi_3, \varphi_7, \varphi_9\}$. And clearly, φ_1 is the identity morphism.

So now we know the elements of $\text{Aut}(G)$, but not the group structure. But we can determine the structure by how the composition of the automorphisms act on 1:

$$\varphi_7 \circ \varphi_7(1) = \varphi_7(\varphi_7(1)) = \varphi_7(7) = \varphi_7(1+1+1+1+1+1+1) = 49 \equiv 9\text{mod}10$$

so $\varphi_7\varphi_7 = \varphi_9$. We can form a Cayley table:

$\text{Aut}(\mathbb{Z}_{10})$	φ_1	φ_3	φ_7	φ_9
φ_1	φ_1	φ_3	φ_7	φ_9
φ_3	φ_3	φ_9	φ_1	φ_7
φ_7	φ_7	φ_1	φ_9	φ_3
φ_9	φ_9	φ_7	φ_3	φ_1

(3) Let $G = D_3$. Let's consider all of the possible inner automorphisms:

$$\{\varphi_e, \varphi_r, \varphi_{r^2}, \varphi_s, \varphi_{sr}, \varphi_{sr^2}\}$$

But we already know that $Z(D_3) = \{e\}$, which you can use to determine that each element of D_3 gives us a nontrivial inner automorphism. From this, you can conclude (with some work) that $\text{Inn}(D_3) \cong D_3$.

We can generalise the second example, but first we need a definition

Definition 6.8. Let $n \in \mathbb{N}$. $(\mathbb{Z}_n)^*$ is defined to be the set of all nonzero numbers coprime to n in $\mathbb{Z}_n$, as a group under multiplication mod$n$. i.e.: as sets, $(\mathbb{Z}_n)^* = \{0 < x < n \mid \gcd(n, x) = 1\}$.

As an exercise, prove that this is a group.

Theorem 6.6. For all $n \in \mathbb{N}$, $\text{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}_n)^*$

Proof. We know that any automorphism of $\mathbb{Z}_n$ is determined by where we send the generator 1, and we know that for it to be an isomorphism we must send it to another generator. From the section on cyclic groups, we know that for a cyclic group $\langle x\rangle$ of order n, the other generators are precisely x^k where $\gcd(k, n) = 1$. Hence, the other generators of $\mathbb{Z}_n$ are $\{k \mid \gcd(k, n) = 1\}$. Let φ_k to be the map from $\mathbb{Z}_n \to \mathbb{Z}_n$ defined by $\varphi_k(1) = k$. Thus, $(\mathbb{Z}_n)^* = \{k \mid \gcd(k, n) = 1\}$, and $\text{Aut}(G) = \{\varphi_k \mid \gcd(k, n) = 1\}$, So these sets are the same size (and finite).

Consider the map $f : \text{Aut}(G) \to (\mathbb{Z}_n)^*$, given by $\varphi_k \mapsto k = \varphi_k(1)$. It is well defined, and one can easily prove that $\varphi_k \circ \varphi_j = \varphi_{kj \mod n}$, meaning $f(\varphi_k\varphi_j) = jk \mod n$, $f(\varphi_k)f(\varphi_j) = kj \mod n$, so it respects the group operation. The kernel is the set of all φ_k such that $f(\varphi_k) = 1$, but by definition, the only one satisfying this is φ_1, the identity. Thus this is a 1-1 map between sets of the same size, and so is a bijection. □

Corollary 6.2. Let p be an odd prime. Then $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$

Proof. If p is a prime, then the numbers $\{1, 2, \ldots, p-1\}$ are all coprime to p. Hence, as a set $(\mathbb{Z}_p)^* = \{1, 2, 3, \ldots, p-1\}$. Let m be the maximal order of the elements under multiplication mod$p$. If G is a finite abelian group, then $|g|$ divides the maximal order for any $g \in G$ (prove as an easy exercise). This means that every $g \in (\mathbb{Z}_p)^*$ is a solution of the equation $x^m - 1 = 0$. By the Fundamental Theorem of Algebra, there are at most m roots, and since each element of $(\mathbb{Z}_p)^*$ is one of them, then $|(\mathbb{Z}_p)^*| \leqslant m$. But we already know by Lagrange's Theorem that the order of a subgroup divides the order of the group meaning m divides $|(\mathbb{Z}_p)^*|$, and so $m \leqslant |(\mathbb{Z}_p)^*|$. Hence, we conclude that $m = |(\mathbb{Z}_p)^*|$, and so it must be cyclic since it has an element whose order is that of the group.
We have $|\mathrm{Aut}(\mathbb{Z}_p)| = |(\mathbb{Z}_p)^*| = p - 1 = |\mathbb{Z}_{p-1}|$. So one has that $\mathbb{Z}_{p-1}$ and $\mathrm{Aut}(\mathbb{Z}_p)$ are finite cyclic groups of the same order, and thus they must be isomorphic. □

7. The Direct Product

We now look into ways of making new groups with groups we already have. The easiest is the direct product (Gallian refers to these as 'external direct products' for reasons beyond my ability to fathom)

Definition 7.1. Let $G_1, G_2, \ldots, G_n$ be groups, with operations $\star_1, \star_2, \ldots, \star_n$ respectively. The *direct product* of these groups is defined as the set of n-tuples $(g_1, g_2, \ldots, g_n)$ with $g_j \in G_j$, and the operation is defined component wise:

$$(g_1, g_2, \ldots, g_n) \star (h_1, h_2, \ldots, h_n) = (g_1 \star_1 h_1,\ g_2 \star_2 h_2,\ \ldots,\ g_n \star_n h_n)$$

The direct product is denoted $G_1 \times G_2 \times \ldots \times G_n$.

Even though there is (potentially) a different operation in each coordinate, we will still use our convention and write

$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1h_1,\ g_2h_2,\ \ldots,\ g_nh_n)$$

Proposition 7.1. If $G_1, \ldots, G_n$ are groups, then $G_1 \times \cdots \times G_n$ is a group of order $|G_1| \cdots |G_n|$.

Proof. Define $G = G_1 \times \cdots \times G_n$. The axioms of a group hold in each G_i, and the operation is defined on G component wise, so it is very easy to check each axiom. As an exercise, prove that the operation defined above is a binary operation. For associativity, we see

$$\begin{aligned}(g_1, g_2, \ldots, g_n)&\big[(h_1, h_2, \ldots, h_n)(k_1, k_2, \ldots, k_n)\big] \\ &= (g_1, g_2, \ldots, g_n)(h_1k_1, h_2k_2, \ldots, h_nk_n) \\ &= (g_1(h_1k_1), g_2(h_2k_2), \ldots, g_n(h_nk_n)) \\ &= ((g_1h_1)k_1, (g_2h_2)k_2, \ldots, (g_nh_n)k_n) \\ &= \big[(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n)\big](k_1, k_2, \ldots, k_n)\end{aligned}$$

The identity element is $e = (e_1, e_2, \ldots, e_n)$, and for inverses, $(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$. The formula for the order of the group is relatively clear, and left as an exercise □

Examples

(1) Let $G = H = \mathbb{Z}_2$. Then $G \times G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (1, 0), (0, 1), (1, 1)\}$, and the operation in each coordinate is addition modulo 2. We can see that each element must have order 2: $(1, 0) + (1, 0) = (1 + 1, 0 + 0) = (0, 0)$, etc. Hence, $\mathbb{Z}_2 \times \mathbb{Z}_2$ has 3 subgroups of order 2. This group is sometimes called the Klein-4 Group.

(2) Consider $\mathbb{Z}_2 \times D_3$. This is the set

$\{(0,e),(0,r),(0,r^2),(0,s),(0,sr),(0,sr^2),(1,e),(1,r),(1,r^2),(1,s),(1,sr),(1,sr^2)\}$

The operation goes as $(n, s^i r^j)(m, s^k r^\ell) = ((n+m)\text{mod}2, s^{i+k} r^{\ell-j})$

(3) For a more general example, and to see that the operations really not have to relate to one another, let $G_1 = \mathbb{Z}_9$, $G_2 = A_5$, and $G_3 = \text{SL}(2,\mathbb{R})$. Then the operation on $G_1 \times G_2 \times G_3$ is

$$\left((n)\text{mod}, \sigma, \begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)\left((m)\text{mod}9, \tau, \begin{bmatrix} x & y \\ z & w \end{bmatrix}\right)$$
$$= \left((n+m)\text{mod}9, \sigma \circ \tau, \begin{bmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{bmatrix}\right)$$

By the way we've constructed the direct product, there is an easy way to compute the order of any element.

Proposition 7.2. Let $g = (g_1, g_2, \ldots, g_n) \in G_1 \times G_2 \times \cdots G_n$. Then the order of g is given by

$$|(g_1, g_2, \ldots, g_n)| = \text{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$$

Proof. For each G_j, let e_j be the identity element. Let $m \in \mathbb{Z}$ such that

$$(g_1, g_2, \ldots, g_n)^m = ({g_1}^m, {g_2}^m, \ldots, {g_n}^m) = (e_1, e_2, \ldots, e_n)$$

This means that for each j, $|g_j|$ divides m. Hence, m must be a common multiple of all the $|g_j|$s. By definition, the smallest is $\text{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$. □

Here is one way we can apply this:

(1) Let $G = \mathbb{Z}_9 \times \mathbb{Z}_3$, and suppose we are asked to determine all of the elements of order 9. Since elements are of the form (n,m), and $|(n,m)| = \text{lcm}(|n|,|m|)$, we need the (n,m) such that $\text{lcm}(|n|,|m|) = 9$. The only ways this is possible is if $|n| = 9$, $|m| = 3$, or $|n| = 9$, $|m| = 1$.

In the first case, the elements of order 9 in $\mathbb{Z}_9$ are 1,2,4,5,7,8. The elements of order 3 in $\mathbb{Z}_3$ are 1,2. This gives us 12 elements of order 9.

In the second case, we still have 1,2,4,5,7,8 as elements of order 9 in $\mathbb{Z}_9$, and there is only one element of order 1 in $\mathbb{Z}_3$, the identity. This gives us an additional 6 elements of order 9. Hence, in total, there are 18 elements of order 9 in $\mathbb{Z}_9 \times \mathbb{Z}_3$.

One of the nicest and easiest classes of groups to deal with is cyclic groups. This next theorem helps us characterise when the product of two cyclic groups is itself cyclic:

Theorem 7.1. Let G, H be finite cyclic groups. The direct product $G \times H$ is cyclic if and only if $\gcd(|G|,|H|) = 1$.

Proof. Let $|G| = a, |H| = b$, so $|G \times H| = ab$. First, suppose $G \times H$ is cyclic; we want to show that $\gcd(a,b) = 1$. Let $d = \gcd(a,b)$, and let $(g,h) \in G \times H$ such that $G \times H = \langle (g,h) \rangle$. We have

$$(g,h)^{ab/d} = ((g^a)^{b/d}, (h^b)^{a/d}) = (e,e)$$

we must have $|(g,h)|$ divides ab/d. But the order of (g,h) is ab, since it generates a cyclic group of order ab. Hence, $d = 1$.

Now, suppose $\gcd(a,b) = 1$. Let g be a generator of G, and h a generator of H. Then

$$|(g,h)| = \text{lcm}(|g|,|h|) = \text{lcm}(a,b) = ab/\gcd(a,b) = ab/1 = ab$$

□

Corollary 7.1. Let G_i be finite cyclic groups. The direct product $G_1 \times \ldots G_n$ is cyclic if and only if $\gcd(|G_i|,|G_j|) = 1$ for all $i \neq j$, each between 1 and n.

Proof. This follows using the previous theorem, and an inductive argument. The details are left as an exercise. □

One of the most important corollaries helps us determine when we can decompose $\mathbb{Z}_n$ as a direct sum of other $\mathbb{Z}_i$.

Corollary 7.2. Let $k = n_1 n_2 \cdots n_m$. Then $\mathbb{Z}_k \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_m}$ if any only if $\gcd(n_i, n_j) = 1$ for $i \neq j$.

Proof. This follows nearly directly from the previous results □

This allows us to see when certain products of $\mathbb{Z}_n$s are the same group. Examples:

(1) $\mathbb{Z}_{18} \cong \mathbb{Z}_2 \times \mathbb{Z}_9$
(2) $\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_6 \cong \mathbb{Z}_4 \times \mathbb{Z}_{10} \times \mathbb{Z}_3 \cong \mathbb{Z}_{12} \times \mathbb{Z}_{10}$
(3) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_{30}$

But notice that $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$.
This theorem will be very important when it comes time to classify finitely generated abelian groups.

8. Quotient Groups, Isomorphism theorems

We're now in a position to combine the knowledge we have about normal subgroups and homomorphisms, and use them to create new groups.

Definition 8.1. Let G be a group, and let H be any subgroup. We use G/H to denote the set of all cosets of H in G : $G/H = \{gH \mid g \in G\}$.

It is important to keep in mind this is generally just a set (of sets).
Up until this point, it has not been clear why normal subgroups are important. Now is this time:

Theorem 8.1. Let G be a group, and let H be a normal subgroup of G. The set of all cosets of H in G, G/H, is group with operation $(gH)(fH) = (gf)H$, for $g, f \in G$. This group is called the *quotient group*; G/H is usually referred to as "G mod H".

Proof. Since H is normal, this means that for every $g \in G$, we have $gH = Hg$.
Cosets can have different representatives, so it is important for us to check that this binary operation is well defined, i.e.: it's the same, no matter which representative we pick. We start with our two cosets, gH, fH, and we choose other representatives for them: $gH = g'H$, and $fH = f'H$. This means that there exists $h_1, h_2 \in H$ such that $g' = gh_1$, and $f' = fh_2$. If we're claiming that $(gH)(fH) = (gf)H$, then it must also be true that $(g'H)(f'H) = (g'f')H = (gf)H$. Remembering that for all $h \in H$, we have $hH = H$, we see:

$$(g'f')H = (gh_1 fh_2)H = (gh_1 f)H = (gh_1)Hf = gHf = (gf)H$$

Hence, the operation is well defined, because it's the same on all representatives.
Now we must show it is a group. The element $eH = H$ is the identity, since $(gH)(eH) = gH$ for all gH. For any gH in G/H, the element $g^{-1}H$ is also in G/H, and this acts as the inverse. Finally, we see

$$(gHfH)kH = (gf)HkH = (gf)kH = g(fk)H = gH(fk)H = gH(fHkH)$$

so the operation is associative. Hence, G/H is a group. □

It turns out the statement of this theorem is actually and "if and only if", since the converse is true

Proposition 8.1. Let G be a group, and H a subgroup such that the set of cosets G/H is a group under the operation defined in theorem 8.1. Then H is normal in G.

Proof. The proof is left as an exercise. □

Let's illustrate with some examples

Examples

(1) Let $G = \mathbb{Z}$, and let $H = 3\mathbb{Z} = \{0, \pm 3, \pm 6, \ldots\}$. To form G/H, we must look at the left cosets of H in G:

$$0 + 3\mathbb{Z} = \{0, \pm 3, \pm 6, \ldots\} = 3\mathbb{Z}$$
$$1 + 3\mathbb{Z} = \{1, 4, -2, 7, -5, \ldots\}$$
$$2 + 3\mathbb{Z} = \{2, 5, -1, 8, -4, \ldots\}$$

In fact, these are all of the cosets. If $n \in \mathbb{Z}$, and $n > 3$, then there exists $q \neq 0$ and $0 \leqslant r < 3$ such that $n = 3q + r$. Thus, the coset $n + 3\mathbb{Z} = r + 3q + 3\mathbb{Z} = r + 3\mathbb{Z}$, since $3q \in 3\mathbb{Z}$. The quotient group is $\mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$, where $(a + 3\mathbb{Z})(b + 3\mathbb{Z}) = (a + b) + 3\mathbb{Z}$, and we see that

$$(1 + 3\mathbb{Z}) + (2 + 3\mathbb{Z}) = (1 + 2) + 3\mathbb{Z} = 3 + 3\mathbb{Z} = 3\mathbb{Z} = 0 + 3\mathbb{Z}$$

If one completes the Cayley table, it can be concluded the operation is effectively addition modulo 3. From this, we can conclude $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$. As an exercise, construct the isomorphism.

(2) Let $G = D_n$, and let $H = \langle r \rangle = \{e, r, r^2, \ldots, r^{n-1}\}$, the subgroup of all of the rotations. We know that $|D_n| = 2n$, and $|H| = n$, thus $[G : H] = 2$, meaning there are 2 left cosets (and that H is normal in G). Hence G/H is a group of order 2, and so must be cyclic (since 2 is a prime).

(3) Let $G = (Z_{15})^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication mod 15. Let H be the group generated by the element 4: $\langle 4 \rangle = \{4, 1\}$, since $4^2 = 16 \equiv 1 \mod 15$. Then $|G/H| = 8/2 = 4$, meaning there are 4 distinct cosets. Listing them:

$$H = \{1, 4\} = 4H$$
$$2H = \{2, 8\} = \{\overline{32}, 8\} = 8H$$
$$7H = \{7, \overline{28}\} = \{7, 13\} = \{\overline{52}, 13\} = 13H$$
$$11H = \{11, \overline{44}\} = \{11, 14\} = \{\overline{56}, 14\} = 14H$$

Where the bar above the numbers bigger than 15 refer to their equivalence class mod 15. If we write out the Cayley table, we see:

	H	$2H$	$7H$	$11H$
H	H	$2H$	$7H$	$11H$
$2H$	$2H$	H	$11H$	$7H$
$7H$	$7H$	$11H$	H	$2H$
$11H$	$11H$	$7H$	$2H$	H

From this table, we see that the group is abelian, and each element is of order 2. One can show that $G/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(4) Let $G = \mathbb{Z}_{84}$,and let $H = \langle 36 \rangle$. Suppose we want to compute $|G/H|$, and also the order of the element $(8 + H)$ in G/H. We know $|1| = 84$, and since the group is additive, this means that $g^n = ng$ for any $g \in G, n \in \mathbb{Z}$.

So $\langle 36 \rangle = \langle 1^{36} \rangle = \langle 1 \cdot 36 \rangle$, and hence $|\langle 36 \rangle| = 84/\gcd(36, 84) = 7$. There may be an easier generator to work with, and since we remember that $\langle 1^{36} \rangle = \langle 1^n \rangle \Leftrightarrow \gcd(84, 36) = \gcd(84, n)$, we get that $n = 12$ is such a number. i.e.: $\langle 36 \rangle = \langle 12 \rangle$ in $\mathbb{Z}_{84}$.

$|G/H| = |G|/|H| = 84/7 = 12$.

For the order of $8 + H$ in G/H, since $(8 + H)^n = 8n + H$, we need an n such that $8n \in H$;

in other words, what is the smallest n such that $8n$ is a multiple of 12 (since $H = \langle 12 \rangle$). Well, $8 \cdot 3 = 24$, and obviously neither $n = 1, 2$ work, so $n = 3$ is the smallest, and hence $|8 + H| = 3$.

(5) Let $G = \mathrm{GL}(n, \mathbb{R})$. The subgroup $\mathrm{SL}(n, \mathbb{R}) = \{A \in \mathrm{GL}(n, \mathbb{R}) \mid \det(A) = 1\}$ is a normal subgroup: let $A \in \mathrm{SL}(n, \mathbb{R})$, and let $B \in \mathrm{GL}(n, \mathbb{R})$. Then $\det(BAB^{-1}) = \det(B)\det(A)/\det(B) = \det(A) = 1$, so $BAB^{-1} \in \mathrm{SL}(n, \mathbb{R})$.

Consider $\mathrm{GL}(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{R})$. Since both groups are infinite, we cannot say anything meaningful about the number of cosets just yet. For brevity, let $H = \mathrm{SL}(n, \mathbb{R})$. We know that two cosets are equal $AH = BH$ if and only if $B^{-1}A \in H$. This means $1 = \det(B^{-1}A) = \det(A)/\det(B)$, which happens if and only if $\det(A) = \det(B)$. Hence, the cosets are indexed by the values of the determinant: each coset only has representatives with the same determinant (so no two cosets are equal if the representatives have different determinants) and hence the cosets are in 1-1 correspondence with the possible values of the determinant. Since the image of the determinant from $\mathrm{GL}(n, \mathbb{R})$ is all of $\mathbb{R}^*$ (why? Answer is given later), this means the cosets are in 1-1 correspondence with $\mathbb{R}^*$.

Let AH, BH be elements of the quotient. Then $(AH)(BH) = (AB)H$. Since $\det(AB) = \det(A)\det(B) = \det(B)\det(A) = \det(BA)$, this means that $(AB)H = (BA)H$: they're representatives of the same coset, since they have the same determinant. This means the quotient group is abelian.

Consider the map $\varphi : \mathrm{GL}(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{R}) \to \mathbb{R}^*$, given by $AH \mapsto \det(A)$. It is surjective, since every element of $\mathbb{R}^*$ is the determinant of some $n \times n$ matrix, and it is injective as we have already proven above. It is also a group morphism, as $\varphi((AB)H) = \det(AB) = \det(A)\det(B) = \varphi(AH)\varphi(BH)$, and as both groups are abelian, this is compatible with their structures. Hence, since φ is a bijective group homomorphism, i.e.: an isomorphism.

$$\mathrm{GL}(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{R}) \cong \mathbb{R}^*$$

8.1. **Applications of Quotient Groups.** For finite groups, the order of a quotient group is smaller than the original group, and its group structure is usually easier to deal with. What is useful about this is that one can often analyze properties of G from properties of G/H. Here are some theorems which illustrate this

Theorem 8.2. Let G be a group, and $Z(G)$ be the centre of G. If $G/Z(G)$ is cyclic, then G is abelian.

Proof. Suppose $G/Z(G)$ is cyclic, and let $gZ(G)$ be a generator. Let $h, k \in G$. Since $G/Z(G)$ is cyclic, there exists integers n, m such that $hZ(G) = (gZ(G))^n = g^n Z(G)$, and $kZ(G) = (gZ(G))^m = g^m Z(G)$. This means that there are $a, b \in Z(G)$ such that $h = g^n a$, and $k = g^m b$. Thus, we are able to compute that

$$\begin{aligned} hk = (g^n a)(g^m b) &= g^n(ag^m)b = g^n(g^m a)b = g^{n+m}ab \\ &= (g^m g^n)ba = g^m(g^n b)a = g^m(bg^n)a = (g^m b)(g^n a) = kh \end{aligned}$$

Hence, $(hZ(G))(kZ(G)) = (hk)Z(G) = (kh)Z(G) = (kZ(G))(hZ(G))$. □

It's important to note from this theorem that if $G/Z(G)$ is cyclic, then G is abelian, which means that $Z(G) = G$, and hence $G/Z(G) = \{e\}$.

Theorem 8.3. Let G be any group. The quotient $G/Z(G)$ is isomorphic to $\mathrm{Inn}(G)$.

Proof. For any $g \in G$, recall that the inner automorphism φ_g is defined as the map from G to itself, by $\varphi_g(x) = gxg^{-1}$. Consider the map $f : G/Z(G) \to \mathrm{Inn}(G)$, $gZ(G) \mapsto \varphi_g$. The first thing to check is that this is actually well defined: suppose $gZ(G) = hZ(G)$. This means that $h^{-1}g \in Z(G)$, and

so $\forall\, x \in G$, we have $(h^{-1}g)x = x(h^{-1}g)$. Rearranging, we get that $gxg^{-1} = hxh^{-1}$ for all $x \in G$, meaning $\varphi_g = \varphi_h$, and so the map f is well defined.
To show 1-1, we just reverse this argument: if we suppose that $\varphi_g = \varphi_h$, then $gxg^{-1} = hxh^{-1}$ for all $x \in G$, meaning $(h^{-1}g)x = x(h^{-1}g)$, which implies $h^{-1}g \in Z(G)$, and so $gZ(G) = hZ(G)$. The map f is clearly surjective (using the fact that if $g \in Z(G)$, then $\varphi_g = \varphi_e$).
As it's easy to check that $\varphi_{gh} = \varphi_g \circ \varphi_h$, this is a group homomorphism. □

What's nice is this allows us to get an idea of the size and structure of $\operatorname{Inn}(G)$ without having to actually compute any inner automorphisms. For example,$Z(S_n) = \{e\}$, meaning $\operatorname{Inn}(S_n) \cong S_n$. As another example, if we consider D_4, we know $Z(D_4) = \{e, r^2\}$. Hence, $|\operatorname{Inn}(G)| = |D_4|/|Z(G)| = 8/2 = 4$. Since 4 is the square of a prime, we could argue that a group of order 4 must either be cyclic, or each non-identity element must have order 2; it is not a large jump to show that the only two possibilities are $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. But if it were $\mathbb{Z}_4$, the quotient would be cyclic which would imply that D_4 is abelian. Since it isn't, we must have $\operatorname{Inn}(D_4) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

8.2. **Quotients and Homomorphisms; the Isomorphism Theorems.** We now relate our work with quotients and homomorphisms, culminating in one of the most important theorems in abstract algebra.

Proposition 8.2. Let G be a group, and let $H \trianglelefteq G$ be a normal subgroup. The map $\pi : G \to G/H$ defined as $\pi(g) = gH$ is a group homomorphism, called the *natural projection* of G onto G/H.

Proof. This map is clearly well defined. It is a group homomorphism because

$$\pi(g_1g_2) = (g_1g_2)H = (g_1H)(g_2H) = \pi(g_1)\pi(g_2)$$

□

This is integral to proving the next proposition. We learned previously that the kernel of any group homomorphism is a normal subgroup. It turns out that the statement is if and only if:

Proposition 8.3. Let G be a group, and let H be a subgroup of G. Then H is normal in G if and only if it is the kernel of an homomorphism.

Proof. We already know one direction. Now, suppose H is normal in G. Consider the natural projection $\pi : G \to G/H$. The kernel of this map is

$$\begin{aligned}\ker\pi &= \{g \in G \,|\, \pi(g) = eH\}\\ &= \{g \in G \,|\, gH = eH\}\\ &= \{g \in G \,|\, g \in H\} = H\end{aligned}$$

Thus, H is the kernel of the natural projection homomorphism π. □

The next theorem is sometimes called "The Fundamental Theorem of Homomorphisms" because of its importance. There are analogues of this theorem in many areas of mathematics.

Theorem 8.4. The First Isomorphism Theorem Let $\varphi : G \to G'$ be a group homomorphism. The quotient of G by the kernel of φ is isomorphic to the image of φ. Formally:

$$G/\ker\varphi \cong \varphi(G) \tag{5}$$

Proof. Consider the map $f : G/\ker\varphi \to \varphi(G)$ defined by $f(g\ker\varphi) = \varphi(g)$. This is well defined because if $g\ker\varphi = h\ker\varphi$, then $h^{-1}g \in \ker\varphi$. Hence, $e = \varphi(h^{-1}g) = \varphi(h)^{-1}\varphi(g)$, and so $\varphi(g) =$

$\varphi(h)$. Reversing this argument shows that the map is 1-1. Showing that this is an homomorphism follows by

$$f(gh\ker\varphi) = \varphi(gh) = \varphi(g)\varphi(h) = f(g\ker\varphi)f(h\ker\varphi)$$

Since every element of G is a representative of some coset, the map is clearly onto. □

Corollary 8.1. Let $\varphi : G \to G'$ be a group homomorphism. Then

1. φ injective iff $\ker\varphi = \{e\}$
2. $[G : \ker\varphi] = |\varphi(G)|$

examples

1. Consider the group homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ defined by $x \mapsto x \mod n$. The kernel of this is clearly $\langle n\rangle$, and since the image is all of $\mathbb{Z}_n$, we have $\mathbb{Z}/\langle n\rangle \cong \mathbb{Z}_n$.
2. Consider the groups $G = (\mathbb{R}^*, \times)$, and $G' = (\mathbb{R}^+, \times)$, the nonzero, and the positive real numbers respectively, both under multiplication. Consider the map $\varphi : G \to G'$, defined as $\varphi(x) = |x|$. The image of this map is all of $\mathbb{R}^+$, since for any $y \in \mathbb{R}^+$, the element $y \in \mathbb{R}^*$ is certainly mapped to it, as $|y| = y$ for any positive real (as sets, $\mathbb{R}^+ \subset \mathbb{R}^*$). We see that this is a group homomorphism because
$$\varphi(xy) = |xy| = |x||y| = \varphi(x)\varphi(y)$$
Since the identity of $\mathbb{R}^+$ is 1, the kernel of φ is all of the elements $x \in \mathbb{R}^*$ such that $\varphi(x) = 1$, meaning $|x| = 1$. The only numbers that do this are 1 and -1. Hence, by the first isomorphism theorem, we have $\mathbb{R}^*/\{1, -1\} \cong \mathbb{R}^+$.
3. Let $G = S_n$, $n > 2$ and let $G' = \{1, -1\}$ under multiplication. Consider the map $\mathrm{sgn} : G \to G'$ defined as
$$\mathrm{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is an even permutation} \\ -1 & \text{if } \sigma \text{ is an odd permutation} \end{cases}$$
This is a group homomorphism because the product of two odd permutations is an even, two even permutations is even, and an odd and an even is an odd permutation. (Write it out explicitly how the homomorphism works) It is also surjective because the identity is even, and any single transposition is odd.
Since the identity of G' is 1, this means the kernel is the set of all of the even permutations, namely $\ker\varphi = A_n$, and thus $S_n/A_n \cong \{1, -1\} \cong \mathbb{Z}_2$.
4. We revisit a previous example: Consider the quotient group $\mathrm{GL}(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{R})$. The map $\det : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^*$ is a group homomorphism. Since the identity of $\mathbb{R}^*$ is 1, this means
$$\ker\det = \{A \in \mathrm{GL}(n, \mathbb{R}) \mid \det(A) = 1\} = \mathrm{SL}(n, \mathbb{R})$$
The image of the determinant is clearly all of $\mathbb{R}^*$: let a be any element of $\mathbb{R}^*$, then the matrix obtained by taking the $n \times n$ identity matrix and multiplying the first row by a is an element of $\mathrm{GL}(n, \mathbb{R})$ whose determinant is a. So by the first isomorphism theorem,
$$\mathrm{GL}(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{R}) = \mathrm{GL}(n, \mathbb{R})/\ker\det \cong \mathrm{Im}(\det) = \mathbb{R}^*$$

Most abstract algebra texts list 3 or 4 isomorphism theorems. I will only list one of the others, and leave the proof (which uses the first isomorphism theorem) as an exercise

Theorem 8.5. The Third Isomorphism Theorem Let G be a group with H, K normal subgroups of G, and H a subgroup of K. Then $K/H \trianglelefteq G/H$, and $(G/H)/(K/H) \cong G/K$.

As a note, the statement just looks like we "cancel" the H, as though we would numbers. The proof is more complicated than that, but it motivates one of the reasons why we use the / to denote a group quotient, as it has (provable) analogies to quotients of numbers.

9. Group Actions

9.1. **Definition, Examples.**

We now get to one of the major "points" of this course: groups acting on sets. Group actions are a fairly ubiquitous thing in mathematics, and can be a powerful tool for proving theorems, as well as determining structures; a common method for studying an algebraic object is by studying how it acts on other structures.

Definition 9.1. Let G be a group, and let X be a set. A (left) *group action* of G on X is a map $G \times X \to X$, taking a pair (g, x) to an element of X called $g.x$. The map satisfies the properties:

(1) $g.(h.x) = (gh).x \qquad$ for all $g, h \in G$, $x \in X$
(2) $e.x = x \qquad$ for all $x \in X$

We say that "G acts on X", and usually denote it $G \circlearrowright X$.

As a note for the first property: on the left hand side, first the group element h acts on x to give a new element of X called $h.x$, and then the element g acts on *this* element of X to give $g.(h.x) \in X$. On the right hand side, the product happens first in the group, the elements g and h combining with the group operation. This new group element acts on the element x in X. As well, we could easily define a *right* group action to be a map from $X \times G \to X$ defined as $(x, g) \mapsto (x.g)$, and all appropriate results.
We will give examples shortly, but there are some important facts to note first:

Proposition 9.1. Let G be a group, and X a set such that $G \circlearrowright X$. For any $g \in G$, there is a map $\sigma_g : X \to X$, defined by $\sigma_g(x) = g.x$.

(1) For any such $g \in G$, σ_g is a permutation of X
(2) The resulting map $G \to S_X$ defined by $g \mapsto \sigma_g$ is a group homomorphism.

Proof.

(1) A permutation is a bijective map from X to itself. The easiest way to show that σ_g is a permutation is to show that it has both a left inverse and a right inverse. (Recall/exercise: a function $f : A \to B$ is injective if and only if it has a left inverse , and surjective if and only if it has a right inverse). Fix a $g \in G$; we claim that $\sigma_{g^{-1}}$ acts as both a left and a right inverse. For all $x \in X$:

$$\begin{aligned}(\sigma_{g^{-1}} \circ \sigma_g)(x) &= \sigma_{g^{-1}}(\sigma_g(x)) \\ &= \sigma_{g^{-1}}(g.x) \\ &= g^{-1}.(g.x) \\ &= (g^{-1}g).x \\ &= e.x = x\end{aligned}$$

If we switch the roles of g and g^{-1}, we see for all $x \in X$ that $(\sigma_g \circ \sigma_{g^{-1}})(x) = x$. Hence σ_g^{-1} is the 2-sided inverse of σ_g for any $g \in G$, meaning σ_g is a permutation of X.

(2) Part 1 showed that $\varphi(g) = \sigma_g$ is an element of S_X. Let $g, h \in G$, then for all $x \in X$:

$$\begin{aligned}(\varphi(g) \circ \varphi(h))(x) &= \sigma_g(\sigma_h(x)) \\ &= g.(h.x) \\ &= (gh).x \\ &= \varphi(gh)(x)\end{aligned}$$

Meaning φ is a group homomorphism, since $\varphi(gh)$ and $\varphi(g) \circ \varphi(h)$ agree as permutations on every element of X.

□

It's also important to note that given a group homomorphism $\varphi : G \to S_X$, this defines a group action on X via $g.x := \varphi(g)(x)$ (an an exercise, check that this actually defines a group action). Hence, group homomorphisms $G \to S_X$ and group actions $G \circlearrowleft X$ are in bijection.

Examples

(1) Let X be any set, and let G be any group. The *trivial* action of G on X is the one such that for all $g \in G$, $x \in X$, we have $g.x = x$. Since this means each group element acts as the identity permutation on X, the resulting homomorphism $\varphi : G \to S_X$ is the trivial homomorphism.

(2) Let G be any group, and let $X = G$ as a set. The group operation on G is a group action of G on itself: for all $g, h, k \in G$, the action defined by $g.k = (gk) \in G$ satisfies $e.k = k$, and $h.(g.k) = h.(gk) = h(gk) = (hg)k = (hg).k$. Using the cancellation law, one can show that this action is a permutation of the elements of G.

(3) The group $\mathrm{GL}(n, \mathbb{R})$ acts on the vector space $\mathbb{R}^n$ via linear transformations. For any $Y \in \mathbb{R}^n$, and any $A, B \in \mathrm{GL}(n, \mathbb{R})$, we have that $A(BY) = (AB)Y$ (and $IY = Y$ for the identity matrix I).

(4) Let X be a set with n elements. The group S_n acts on X via permutations: $\sigma.x = \sigma(x)$.

(5) Let G be a group with a normal subgroup H. Then G acts on G/H via $g.(kH) = (gk)H$. We have $\forall g, f, k \in G$

$$g.(f.(kH)) = g.(fkH) = g(fk)H = (gf)kH = (gf).(kH); \qquad e.(kH) = kH$$

To see that this action is well defined, let $kH \in G/H$, and let k' be another representative of kH. This means that there exists an $h \in H$ such that $k' = kh$. What we want to show is that for any $g \in G$, $g.(kH) = g.(k'H)$. This would be true if and only if $(gk')^{-1}(gk) \in H$. Since $k' = kh$, we have

$$(gk')^{-1}gk = (gkh)^{-1}gk = (h^{-1}k^{-1}g^{-1})gk = h^{-1}k^{-1}k = h^{-1} \ \in H$$

Hence, $(gk)H = (gk')H$, so this action is well defined.

(6) Let G be a group. The group $\mathrm{Aut}(G)$ acts on G in the obvious way: for all $\varphi \in \mathrm{Aut}(G)$, $g \in G$, $\varphi.g = \varphi(g)$. (as an exercise, verify that this is a group action).

(7) In particular, the inner automorphisms act on G. Since the inner automorphisms are indexed by the elements of G, this amounts to saying that G acts on itself by conjugation. For all $g, h, k \in G$:

$$\varphi_g.h = \varphi_g(h) = ghg^{-1}; \qquad \varphi_e(h) = ehe^{-1} = h$$
$$\varphi_k.(\varphi_g.h) = \varphi_k(\varphi_g(h)) = \varphi_k(ghg^{-1}) = kghg^{-1}k^{-1} = \varphi_{kg}(h) = \varphi_{kg}.h$$

(8) Let $G = D_n$, and let X be the set of vertices of a regular n-gon. Then D_n acts on X via the symmetries D_n describes.

9.2. **Orbits, Stabilisers.** Given a group action of G on X, we can put an equivalence relation on X: $x \sim y$ if and only if there exists a $g \in G$ such that $g.x = y$. Let's prove that it is an equivalence relation:

(1) **Reflexivity** Since for any $x \in X$ we know that $e.x = x$, we have $x \sim x$.

(2) **Symmetry** Suppose that $x \sim y$. This means that there exists a $g \in G$ such that $g.x = y$. Acting by g^{-1}, we see $g^{-1}.y = e.x = x$, and so $y \sim x$.

(3) **Transitivity** Suppose that $x \sim y$, and $y \sim z$. This means there exists $g, h \in G$ such that $g.x = y$, and $h.y = z$. This means that $(hg).x = h.(g.x) = h.y = z$, and so $x \sim z$.

This means that the group action partitions X into a disjoint union of equivalence classes.

Definition 9.2. Orbit Let $G \circlearrowright X$. For a point $x \in X$, we denote its equivalence class induced by the group action by $\mathcal{O}(x) = \{g.x \,|\, g \in G\}$. This equivalence class is called the "orbit through x".

This leads us to define a special kind of group action

Definition 9.3. Transitive Group Action Let $G \circlearrowright X$. Suppose that there is only one orbit; in other words, for any $x \in X$, $\mathcal{O}(x) = X$. Then the group action is called a *transitive action.* This condition is equivalent to saying that for any $x, y \in X$, there exists a $g \in G$ such that $g.x = y$.

A transitive action on X basically means that given any starting point in X, you can "get to" anywhere else in X via the group action.

Definition 9.4. Stabiliser Let $G \circlearrowright X$. For any $x \in X$, define the *stabiliser* of x to be

$$G_x = \{g \in G \,|\, g.x = x\}$$

In other words, all of the elements of G which fix x. The stabiliser is also sometimes denoted $\text{stab}(x)$.

Orbits and stabilisers are very important to group actions, and are usually talked about closely together. It is worth remembering, though that the orbits live in X, and the stabilisers live in G.

Proposition 9.2. If $G \circlearrowright X$, then for any $x \in X$, the stabiliser of x is a subgroup of G.

Proof. Let $g, h \in G_x$. Then $g.x = x$, and $h.x = x$. This also means that $x = h^{-1}.x$. Hence, we see that

$$(gh^{-1}).x = g.(h^{-1}.x) = g.x = x$$

Since $e.x = x$ always, this means G_x is nonempty. Thus, by the one-step subgroup test, we have that G_x is a subgroup of G. □

Let us look at some examples

(1) Let $G = D_n$, and X the set of vertices of a regular n-gon. Pick some vertex x: the orbit through x is all of X, since x can be sent to any other vertex using an appropriate rotation. Hence, this group action is transitive. The stabiliser of x is the 0 rotation (the identity), and the reflexion through x, meaning for any $x \in X$, $G_x \cong \mathbb{Z}_2$.

(2) Let $G \circlearrowright X$ be the trivial action: $g.x = x$ for all $g \in G$, $x \in X$. Then the number of distinct orbits is $|X|$, since each orbit has only one element in it (namely, x for any $x \in X$). Since every element of G fixes any x, this means $G_x = G$ for all $x \in X$.

(3) Let G act on itself via conjugation. For any $h \in G$, the orbit through h is

$$\mathcal{O}(h) = \{ghg^{-1} \,|\, g \in G\}$$

which is called the *conjugacy class of* h (which we will see later on). The stabiliser of any h is

$$G_h = \{g \in G \,|\, ghg^{-1} = h\} = \{g \in G \,|\, gh = hg\} = C(h)$$

The centraliser of h.

(4) Let $G = O(n) = \{A \in \text{GL}(n, \mathbb{R}) \,|\, AA^T = A^TA = I\}$. This is a subgroup of $\text{GL}(n, \mathbb{R})$, and so acts on $\mathbb{R}^n$. The matrices in $\text{GL}(n, \mathbb{R})$ preserve lengths of vectors in the standard metric, as for any $Y \in \mathbb{R}^n$, we have

$$||AY|| = \sqrt{\langle AY, AY \rangle} = \sqrt{\langle A^TAY, Y \rangle} = \sqrt{\langle IY, Y \rangle} = \sqrt{\langle Y, Y \rangle} = ||Y||$$

Hence, the orbits of $O(n)$ are spheres centred at the origin (note: there is a difference between a 'sphere' and a 'ball'. The former is 'hollow', the latter is filled in. So the 2-sphere of radius r in $\mathbb{R}^3$ is the set of all points (x, y, z) which satisfy $x^2 + y^2 + z^2 = r^2$. The (closed)

ball of radius r in $\mathbb{R}^3$ is the set of points (x, y, z) satisfying $x^2 + y^2 + z^2 \leqslant r^2$. A 1-sphere in $\mathbb{R}^2$ is a circle. A ball in $\mathbb{R}^2$ is a disc).
For any $Y \in \mathbb{R}^n$, the stabiliser of Y is all of the $A \in O(n)$ such that $AY = Y$, namely all of the matrices who have Y as an eigenvector with eigenvalue 1.

(5) Let G be a group, and H a normal subgroup; G acts on the quotient group G/H. Let kH be an element of G/H. The orbit through kH is all of G/H: for any $fH \in G/H$, there exists a $g \in G$ such that $g.kH = fH$, namely, $g = fk^{-1}$. Hence, there is one orbit, and so $G \circlearrowright G/H$ is transitive. The stabiliser of kH is the set of all $g \in G$ such that $g.kH = kH$, meaning $(gk)H = kH$. This is true if and only if $k^{-1}gk = h \in H$, meaning $g = khk^{-1}$. But since H is normal, this means $khk^{-1} = h' \in H$, and so $g \in H$. Hence, $G_{kH} = H$.

(6) Let G be a group, and let H be *any* subgroup. Now, G/H isn't necessarily a group (unless H is normal), it is just a set of cosets. G still acts on G/H via $g.(kH) = (gk)H$ for any $g, k \in G$. This action is still transitive: given any two elements of G/H, kH, and jK for $k, j \in G$, there exists a $g \in G$ such that $g.(kH) = jH$, namely, $g = jk^{-1}$. The stabilisers are a little more complicated: for any kH, the stabiliser is $G_{kH} = \{g \in G \,|\, (gk)H = kH\}$ as before, but since H isn't necessarily normal, we can't use the same conjugation deduction. What we get instead is that if $(gk)H = kH$, then there exists a $h \in H$ such that $k^{-1}gk = h$, meaning $g = khk^{-1}$. In fact, if we pick any $h \in H$ and conjugate by k, we'll get a group element which will stabilise kH, and so can conclude that $G_{kH} = kHk^{-1}$ for any $k \in G$.

In fact, we can generalise the last example

Proposition 9.3. Let $G \circlearrowright X$, and let x, y be in the same orbit (i.e.: $\exists g \in G$ such that $g.x = y$). Then the stabilisers are related by $G_y = gG_xg^{-1}$

Proof. By definition $G_x = \{h \in G \,|\, h.x = x\}$, and $G_y = \{k \in G \,|\, k.y = y\}$. Since $y = g.x$, this means

$$\begin{aligned} G_y &= \{k \in G \,|\, k.(g.x) = g.x\} \\ &= \{k \in G \,|\, (g^{-1}kg).x = x\} \\ &= \{gk'g^{-1} \in G \,|\, k'.x = x\} \qquad\qquad \text{with } k' = g^{-1}kg \\ &= gG_xg^{-1} \end{aligned}$$

□

In examples 5 and 6 above, there is only one orbit, and hence we can relate the stabilisers of any two elements.

Definition 9.5. Let G be a group and X a set such that $G \circlearrowright X$. If $G_x = \{e\}$ for all $x \in X$, then the action is called a *free action.* Equivalently, if there is an $x \in X$ such that $g.x = h.x$, then this implies $g = h$.

We haven't seen too many group actions so far which are free. Here are two examples

(1) Let G act on itself by left multiplication. If $x \in G$, then $G_x = \{g \in G \,|\, g.x = x\}$. But we know that the only group element that does this is e.

(2) Let $G = \mathbb{Z}_2$, and let X be the unit 2-sphere in $\mathbb{R}^3$ centred at the origin (i.e.: $X = \{(x, y, z) \,|\, x^2 + y^2 + z^2 = 1\}$). $\mathbb{Z}_2 \circlearrowright X$ in the following way: the element $1 \in \mathbb{Z}_2$ takes each point, and sends it to the point diametrically opposed to it: $1.(x, y, z) = (-x, -y, -z)$. This is called the *antipodal map.* The identity $0 \in \mathbb{Z}_2$ obviously fixes everything, as per the definition of group action. If the element $1 \in \mathbb{Z}_2$ fixed a point, we would have $(x, y, z) = 1.(x, y, z) = (-x, -y, -z)$, which would imply $x = y = z = 0$, but the origin

(0,0,0) is not on the sphere. Hence, each point only has $0 \in \mathbb{Z}_2$ as the stabiliser, and hence the action is free.

Theorem 9.1. Orbit-Stabiliser Theorem Let G be a group, and X be a set with a G action. Then for any $x \in X$

$$|G/G_x| = |\mathcal{O}(x)|$$

Proof. The way to show two sets are the same size is to create a bijection between them. G/G_x is the set of cosets of the stabiliser of x in G. Consider the map from $G/G_x \to \mathcal{O}(x)$, $gG_x \mapsto g.x$. This is well defined, since if $gG_x = hG_x$, then $h^{-1}g \in G_x$, meaning $(h^{-1}g).x = x$ if and only if $g.x = h.x$. Reversing this argument shows that the map is injective.
Since the orbit is the collection of all such $g.x$, this map must be surjective since every $g \in G$ is a representative of some coset. □

Corollary 9.1. Finite Orbit-Stabiliser Let G be a finite group, and X a finite set such that $G \circlearrowleft X$. Then for any $x \in X$, $|G| = |G_x||\mathcal{O}(x)|$.

Revisiting some examples

(1) Let D_4 act on the the vertices of the square, and let x be any vertex. We already know that the orbit of x is all of the vertices, meaning $|\mathcal{O}(x)| = 4$. The stabiliser is the 0 rotation and the reflexion through x, meaning $|G_x| = 2$. Hence, $|\mathcal{O}(x)||G_x| = (4)(2) = 8 = |D_4|$
(2) Let G be a group of size n, acting on X via the trivial action. For any $x \in X$, $G_x = G$, and $\mathcal{O}(x) = x$, hence, $|\mathcal{O}(x)||G_x| = 1|G| = |G|$
(3) Let G finite, $H \trianglelefteq G$ finite, and let $G \circlearrowleft G/H$. We've shown that for any xH, the stabiliser $G_{xH} = H$. Hence, the size of the orbit of xH is $|\mathcal{O}(xH)| = |G|/|H| = |G/H|$ (which we knew, since we showed the action was transitive).

Corollary 9.2. Let G be a group, and let X be a set such that $G \circlearrowleft X$ transitively. There exists a bijection between X the set of cosets G/G_x for any $x \in X$.

Proof. Since $G \circlearrowleft X$ transitively, this means that there is one orbit. So for any $x \in X$, $\mathcal{O}(x) = X$. Hence, by the orbit stabiliser theorem, $|G/G_x| = |\mathcal{O}(x)| = |X|$. Hence, the map $f : G/G_x \to X$ defined by $gG_x \mapsto g.x$ is a bijection. □

This last corollary we will use to make a slightly stronger statement soon.

9.3. Invariant Subsets, Invariant Elements, Burnside's Lemma.

Burnside's Lemma is a very powerful combinatoric tool that is useful for solving problems.

Definition 9.6. Let G be a group acting on set X. If $Y \subseteq X$, we say *Y is invariant under the action of G* if for every $y \in Y$ and $g \in G$, $g.y \in Y$.

Examples

(1) Let $O(3)$ act on $\mathbb{R}^3$ by linear transformations. The 2-spheres centred at the origin (i.e.: the set of points (x, y, z) satisfying $x^2 + y^2 + z^2 = r^2$ for each $r \in \mathbb{R}$) are invariant under the action, since $O(n)$ preserves lengths.
(2) Let $G \circlearrowleft X$ be any action. Fix an $x \in X$. The orbit of x is $\mathcal{O}(x) = \{g.x \,|\, g \in G\}$. If we take any element of $\mathcal{O}(x)$, and act by an element of G, we get something in $\mathcal{O}(x)$ again: $h.(g.x) = (hg).x$, and since $(hg) \in G$, we clearly have $(hg).x \in \mathcal{O}(x)$ by definition. Hence, the orbits of the group action are invariant subsets.
(3) Let G be any group, and let G act on itself by conjugation. Then the centre, $Z(G)$, is stable under this group action. In fact, it satisfies a stronger condition: for every $x \in Z(G)$, and for every $g \in G$, we have $g.x = gxg^{-1} = x$.

(4) Let X be the unit 2-sphere in $\mathbb{R}^3$, and let $G = S^1 = \{e^{i\theta} \mid \theta \in [0, 2\pi)\}$, the circle group. Pick an equator for the sphere, and let G act on X via rotation through the poles (so $e^{i\theta}$ rotates the sphere about the poles by an angle of θ). The set $Y = \{NP,\ SP\}$ of the 'north' and 'south' poles is invariant under the action, since $e^{i\theta}.NP = NP$ for all θ, and similarly for SP.

These last two examples leads us to the following definition:

Definition 9.7. Let G, a group, act on X, a set. An element $x \in X$ is said to be *invariant under the group action*, or *G-invariant* if for all $g \in G$, $g.x = x$. The set of all G-invariant elements is denoted X^G.

An important thing to note is that the set of invariant elements X^G is an invariant subset per definition 10.6, but the reverse isn't true: an invariant subset of X does not necessarily have each element being invariant.
Examples

(1) Using the previous examples, S^1 acting on the 2-sphere, the poles are precisely the fixed point sets. All other points on the sphere rotate, but only the poles are fixed by every group element. Hence, $X^{S^1} = \{NP, SP\}$.
(2) If G acts on itself by conjugation, the fixed point set is defined to be

$$X^G = \{x \in G \mid \forall g \in G,\ gxg^{-1} = x\} = \{x \in G \mid \forall g \in G,\ gx = xg\} = Z(G)$$

(3) Let $G \circlearrowright G/H$, where H is any subgroup. Since this action is transitive, no element is fixed by the whole group (since for every kH, jH, there exists a $g \in G$ such that $g.(kH) = jH$). Hence, $X^G = \varnothing$ (or more accurately, $(G/H)^G = \varnothing$).

Relaxing the conditions a bit, we can define

Definition 9.8. Let $G \circlearrowright X$. For each $g \in G$, define X^g to be the set of all elements of X which are fixed by the element g.

$$X^g = \{x \in X \mid g.x = x\}$$

So instead of looking at the points in X fixed by *all* of G, we can look at the points fixed by just one element of G. This is a similar concept to the stabiliser of a point, but they live in different places. For an $x \in X$, the stabiliser is a set of elements of G which stabilise x. For a $g \in G$, the fixed points of the permutation induced by g is a set of elements of X which g fixes. Hence, $G_x \subseteq G$, and $X^g \subseteq X$.
Examples

(1) Let $G = D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$, and let X be the vertices of the square. The fixed point set of the rotation r is nothing, since it permutes all of the vertices; $X^r = \varnothing$. Number the vertices 1,2,3,4, and let s be the reflexion whose axis goes through the vertices $1, \& 3$. The fixed point set of this element is the vertices $1, 3$ since they do not change with the reflexion; $X^s = \{1, 3\}$.
(2) Let G act on $X = G/H$, where H is a normal subgroup of G. Let h be any element of H. This means that for any $gH \in G/H$, we have $h.(gH) = (hg)H = hHg = Hg = gH$, so all points are fixed by h. Hence $X^h = X = G/H$.
(3) Let $G = S_9$, acting on the set $X = \{1, 2, \ldots, 9\}$ and let $\sigma = (1256)$. Then clearly $X^\sigma = \{3, 4, 7, 8, 9\}$.

These definitions, together with the orbit-stabiliser theorem, lead us to a very important theorem called 'Burnside's Lemma', even though Burnside didn't discover it.

Lemma 9.1. Burnside's Lemma Let G be a finite group acting on a set X. Let X/G denote the set of orbits of the group action. Then

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

The proof, while not overly difficult, involves playing around with summations, exchanging some for others. The power of Burnside's Lemma mostly relies in that it is much easier to compute fixed point sets than it is to compute orbits. Here is a basic example

(1) Let S_4 act on $X = \{1, 2, \ldots, 4\}$. For any $\sigma \in S_4$ written in disjoint cycle form, the fixed points of σ are the elements of X not appearing in the cycles of σ. The elements of S_4 are of the following types: the identity, a transposition, a product of transpositions, 3-cycles, and 4-cycles. Any given transposition of S_4 fixes 2 elements, and there are 6 possible transpositions. The product of transpositions and the 4-cycles include all 4 elements, meaning they fix nothing. The 3-cycles fix 1 element each, and there are 8 of them. Hence, by Burnside's

$$\begin{aligned}|X/S_4| &= \frac{1}{4!}\sum_{\sigma\in S_4}|X^\sigma| \\ &= \frac{1}{24}\left(|X^e| + 6|X^{(12)}| + 8|X^{(123)}|\right) \\ &= \frac{1}{24}\left(4 + 6(2) + 8(1)\right) \\ &= \frac{1}{24}(24) \\ &= 1\end{aligned}$$

Meaning there is 1-orbit, and hence the action is transitive (which we already knew)

We'll see a few more combinatorial examples near the end of the course.

9.4. **Equivariant Maps.** Given two sets X, and Y, we can easily make maps between them. But if we have a group G acting on both X and Y, it would be natural to want maps between the sets which also take into account the action structure, just as morphisms of groups take into account the group structure.

Definition 9.9. Let G be a group, and let X and Y be sets such that $G \circlearrowright X$, and $G \circlearrowright Y$. To distinguish, let . denote the action on X, and $*$ the action on Y. A map of sets $f : X \to Y$ is said to be *equivariant* with respect to the group actions if for all $g \in G$, and $x \in X$,

$$f(g.x) = g * f(x)$$

With an equivariant map, it effectively doesn't matter the order in which you do things: you could take the element x in X, act some $g \in G$ on it and then map it with f, or you could map x with f first, and then act the group element on it.

Examples

(1) Let $X = Y = S^1$, the unit circle in $\mathbb{R}^2$ centred at the origin, and let G be the set of rotations of S^1. Let $f : X \to Y$ be the antipodal map: $f(x, y) = (-x, -y)$. Then this map is equivariant with respect to the group action: if g is a rotation by θ, then $g.(x, y) = (\cos\theta x - \sin\theta y, \sin\theta x + \cos\theta y)$. This g can be represented by a rotation matrix. Since the

antipodal map is just multiplication by (-1), we can easily see that

$$\begin{aligned} f(g.x) &= f(\cos\theta x - \sin\theta y, \sin\theta x + \cos\theta y) \\ &= (-\cos\theta x + \sin\theta y, -\sin\theta x - \cos\theta y) \\ &= (\cos\theta(-x) - \sin\theta(-y), \sin\theta(-x) + \cos\theta(-y)) \\ &= g.(-x, -y) \\ &= g.f(x, y) \end{aligned}$$

(2) Let $X = \mathbb{R}^3 \setminus \{0\}$ $Y = S^2$ the unit 2-sphere in $\mathbb{R}^3$, and let $G = O(3)$. Let $f : X \to Y$ defined as $f(v) = \frac{1}{||v||}v$. Since for any $A \in O(3)$ and any $v \in \mathbb{R}^3$, $||Av|| = ||v||$, this map is equivariant with respect to the $O(3)$ actions: $f(Av) = \frac{1}{||Av||}(Av) = \frac{1}{||v||}Av = A(\frac{1}{||v||}v) = Af(v)$.

9.5. **Conjugacy Classes, The Class Equation.** In this section we look at a group action of particular import: a group acting by conjugation. We have already seen that this is a group action, and determined the orbits and stabilisers: $\mathcal{O}(x) = \{gxg^{-1} \mid g \in G\}$, and $G_x = \{g \in G \mid gx = xg\} = C_G(x)$. The stabiliser of an element under this action is the centraliser of the element, and the orbit of an element x is called the *conjugacy class of x*.

Definition 9.10. Let G be a group. Two elements $x, y \in G$ are called *conjugate in G* if $\exists g \in G$ such that $x = gyg^{-1}$. This is true if and only if x and y are in the same orbit of the conjugation action.

(1) If G is abelian, then the conjugation action is trivial. This means that for any element $x \in G$, we have $G_x = C_G(x) = G$, and the conjugacy class of x is $\mathcal{O}(x) = \{x\}$, since $gxg^{-1} = x$ for all g.
(2) Let $G = D_3$. We can compute directly that the conjugacy classes are $\{e\}$, $\{r, r^2\}$, and $\{s, sr, sr^2\}$

An important thing to note is that a group element x is the only member of its orbit if and only if it is in the centre: $\mathcal{O}(x) = \{x\}$ if and only if $gxg^{-1} = x$ for all $g \in G$ if and only if $xg = gx$ for every $g \in G$ if and only if $x \in Z(G)$.
If G is a finite group, then by the orbit-stabiliser theorem we know that given an element $x \in G$, the number of conjugates of it (i.e.: the size of the orbit of x) is equal to $|G|/|G_x| = |G|/|C_G(x)| = [G : C_G(x)]$.

Theorem 9.2. The Class Equation Let G be a finite group. Then

$$\begin{aligned} |G| = &\sum_{g \in G} [G : C_G(g)] \\ =&|Z(G)| + \sum_{g_i} [G : C_G(g_i)] \end{aligned}$$

Where the g_i are representatives of distinct conjugacy classes which are not in the centre.

Proof. Let $Z(G) = \{e, x_2, x_3, \ldots, x_m\}$; each of these elements gives a single-element conjugacy class, as noted above. Let $\mathcal{D}_1, \ldots, \mathcal{D}_j$ be the other conjugacy classes of G (i.e.: of elements not in the centre), and let g_i be a representative of the class $\mathcal{D}_i$. Then all of the conjugacy classes of G are

$$\{e\}, \{x_2\}, \ldots, \{x_m\}, \mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_j$$

As the orbits of a group action induce an equivalence class, the group is a disjoint union of the orbits. Hence,

$$\begin{aligned} |G| &= \sum_{i=1}^{m} 1 + \sum_{i=1}^{j} |\mathcal{D}_i| \\ &= |Z(G)| + \sum_{i=1}^{j} [G : C_G(g_i)] \end{aligned}$$

□

This theorem is a very powerful tool for figuring out structure in finite groups. Two immediate and related consequences are

Proposition 9.4. Let p be a prime, and let G be a group such that $|G| = p^n$ for some $n \in \mathbb{N}$. Then $|Z(G)| > 1$

Proof. Using the Class equation, we have for each g_i (non-centre conjugacy class representative) $[G : C_G(g_i)] = |G|/|C_G(g_i)| = p^k > 1$ for some $k \in \mathbb{N}$, since $|G| = p^n$, and the only elements such that $|C_G(g_i)| = 1$ is for the elements in the centre. If we rearrange the equation:

$$|Z(G)| = |G| - \sum_{g_i} [G : C_G(g_i)]$$

Then p divides $|G|$, and p divides each of the elements of the summand, so p divides the right side of the equation. Hence, p divides $|Z(G)|$, meaning $|Z(G)| > 1$ □

This allows us to classify a certain kind of finite group

Corollary 9.3. Let p be a prime, and G a group such that $|G| = p^2$. Then G is abelian.

Proof. Since $|Z(G)| > 1$ by the previous proposition, and $Z(G)$ is a subgroup, this means $|Z(G)| = p$ or $|Z(G)| = p^2$. If $|Z(G)| = p^2$, then $Z(G) = G$, and so the group is abelian.
If $|Z(G)| = p$, then $|G/Z(G)| = p$, which must mean that $G/Z(G)$ is cyclic, which means G is abelian. □

9.6. **Conjugacy Classes in the Symmetric Groups.** The orbits of the conjugation action of S_n on itself turn out to be very easy to describe.

Proposition 9.5. Let $\sigma, \tau \in S_n$, and suppose $\sigma = (a_1 a_2 \cdots a_k)(b_1 \cdots b_j) \cdots$ in disjoint cycle form. Then $\tau\sigma\tau^{-1} = (\tau(a_1)\tau(a_2) \cdots \tau(a_k))(\tau(b_1) \cdots \tau(b_j)) \cdots$; in other words, σ and $\tau\sigma\tau^{-1}$ have the same cycle decomposition.

Proof. Suppose that $x, y \in \{1, 2, \ldots, n\}$ such that $\sigma(x) = y$. Then

$$\tau\sigma\tau^{-1}(\tau(x)) = \tau\sigma(x) = \tau(y)$$

Hence, if $(xy\ldots)$ appears anywhere in the cycle decomposition of σ, then $(\tau(x)\tau(y)\ldots)$ is in the cycle decomposition of $\tau\sigma\tau^{-1}$. □

This theorem would lead us to think that the conjugacy class of any permutation of S_n is possibly just the collection of all other permutations with the same cycle type. We have proven conjugate implies same cycle type, so all we have left is to verify the converse; luckily, it is also true.

Proposition 9.6. Two elements of S_n are conjugate if and only if they have the same cycle decomposition.

Proof. Let $\sigma, \tau \in S_n$ such that both have the same cycle types. List the cycles in each in increasing order of cycle lengths, including the length-1 cycles (i.e.: the fixed points). Since we've put the permutations in disjoint cycle form, the cycles are a list of all of the numbers from 1 to n in some order, with each number appearing exactly once. Define a map $f : \sigma \to \tau$ which maps the j^{th} number in σ to the j^{th} in τ. Hence, f is a permutation of the elements $\{1, 2, \ldots, n\}$. By our construction, we have $f\sigma f^{-1} = \tau$, meaning σ and τ are conjugate by the previous proposition. □

Examples

(1) Let $\sigma = (6)(13)(245)$, and let $\tau = (1)(45)(236)$. Then $f(6) = 1$, $f(1) = 4$, $f(3) = 5$, $f(2) = 2$, $f(4) = 3$ and $f(5) = 6$. Hence, $f = (14356)(2)$, and $f\sigma f^{-1} = \tau$.

(2) $\sigma = (123)(45)$ and $\tau = (43)(125)$. Since they are the same cycle type, σ and τ are conjugate.

If n is a number, the *partitions* of n are the ways we can split up n as a sum of other numbers. So for example, we can split up 4 as $1 + 1 + 1 + 1$, or $1 + 1 + 2$, or $1 + 3$, or 4, or $2 + 2$.

Proposition 9.7. The number of conjugacy classes of S_n is equal to the number of partitions of n.

Proof. As per the previous proposition, the conjugacy classes of S_n are indexed by the possible cycle types, which themselves are in bijection with the partitions of n: including fixed points, the numbers making up the cycle type add up to n, and for each partition, we can construct an element of S_n with that cycle type by filling in the parentheses with lengths as described by the partition. □

examples

(1) For S_4, we saw above that there were 5 partitions. We can find representatives of each conjugacy class based on the partitions: $1+1+1+1 \mapsto (e)$, $1+1+2 \mapsto (12)$, $1+3 \mapsto (123)$, $4 \mapsto (1234)$, $2+2 \mapsto (12)(34)$.

(2) For S_5, there are seven partitions of 5: 1+1+1+1+1, 1+1+1+2, 1+1+3, 1+4, 5, 2+3, 1+2+2. These respectively correspond to the conjugacy classes with representatives e, (12), (123), (1234), (12345), (12)(345), (12)(34).

10. Semi-Direct Products

The easiest way we saw to combine two groups G and G' was to form the direct product, the set of pairs of elements where the group multiplication happened componentwise. In this case, the two individual groups making up the product did not 'interact' in any way. With a little added structure, we can form a new group where the individual groups do interact, however.

Definition 10.1. Let H and K be groups, and let $\varphi : K \to \operatorname{Aut}(H)$ be a group homomorphism. For ease of notation, let $\varphi_k := \varphi(k)$ for any $k \in K$. The *semi-direct product* of H and K as a set is the collection of ordered pairs $(h, k) \in H \times K$, with operation defined as follows:

$$(h_1, k_1)(h_2, k_2) = (h_1\varphi_{k_1}(h_2), k_1k_2)$$

The semi-direct product is denoted $H \rtimes_\varphi K$, or sometimes $H \rtimes K$ if there is no confusion about the homomorphism.

Since $\varphi_k \in \operatorname{Aut}(H)$, this means $\varphi_k(h_2) = h'$ for some $h' \in H$. Hence, $h_1\varphi_{k_1}(h_2) = h_1h'$, the group product of h_1 and h' in H.

This group homomorphism $K \to \operatorname{Aut}(H)$ gives us a group action of K on H by group automorphisms. Hence, we could write the multiplication as $(h_1, k_1)(h_2, k_2) = (h_1(k_1.h_2), k_1k_2)$ where . denotes the group action via the automorphism. We prefer to keep the φ unless there is no confusion of which homomorphism is being used.

Proposition 10.1. Let H and K be groups, with a group homomorphism $\varphi : K \to \operatorname{Aut}(H)$. Then

(1) The semi-direct product $G = H \rtimes K$ is a group of order $|H||K|$
(2) H and K are isomorphic to subgroups of $H \rtimes K$: $H \cong \{(h, e_K) \,|\, h \in H\}$, and $K \cong \{(e_H, k) \,|\, k \in K\}$.
(3) $H \trianglelefteq G$

Proof.

(1) The identity is (e_H, e_K), the inverse is $(h,k)^{-1} = (\varphi_{k^{-1}}(h^{-1}), k^{-1})$, and the multiplication is associative. Verifying these is straightforward, and left as an exercise.
Since G as a set is $H \times K$, then $|G| = |H||K|$.
(2) For $(h_1, e_K), (h_2, e_K) \in G$, we have
$$(h_1, e_K)(h_2, e_K) = (h_1\varphi_{e_K}(h_2), e_K) = (h_1h_2, e_K)$$
Similarly, for $(e_H, k_1), (e_H, k_2) \in G$, we have
$$(e_H, k_1)(e_H, k_2) = (e_H, k_1k_2)$$
This shows the maps $H \to G$, $h \mapsto (h, e_K)$, $K \to G$, $k \mapsto (e_H, k)$ are injective group morphisms.
(3) Let $(h, e_K) \in H \subset G$, and let (h', k) be any element of G. Then
$$\begin{aligned}(h', k)(h, e_K)(h', k)^{-1} &= (h', k)(h, e_K)(\varphi_{k^{-1}}(h'^{-1}), k^{-1}) \\ &= (h'\varphi_k(h), k)(\varphi_{k^{-1}}(h'^{-1}), k^{-1}) \\ &= ([h'\varphi_k(h)]\varphi_k(\varphi_{k^{-1}}(h'^{-1})),\ kk^{-1}) \\ &= (h'\varphi_k(h)h'^{-1},\ e_K) \in H \subset G\end{aligned}$$

□

This last part helps to justify the notation to a degree: as a set, the semi-direct product is $G = H \times K$, and in the semi-direct product, $H \trianglelefteq G$, so together we get $G = H \rtimes K$.

Examples

(1) Let H be an abelian of group of any order, and let $K \cong \mathbb{Z}_2$. Let $\varphi : \mathbb{Z}_2 \to \mathrm{Aut}(H)$ be defined by 1 maps to the automorphism which takes an element to its inverse. i.e.: $\varphi_1(h) = h^{-1}$ for any $h \in H$. Then in $G = H \rtimes \mathbb{Z}_2$, for any $h_1, h_2 \in H$, we have the multiplication
$$(h_1, 1)(h_2, 0) = (h_1{h_2}^{-1}, 1); \qquad (h_1, 0)(h_2, 0) = (h_1h_2, 0), \text{ etc}$$
(2) Let A be a matrix in $\mathrm{GL}(n, \mathbb{R})$ in the following block form:
$$A = \begin{pmatrix} 1 & X^T \\ 0 & B \end{pmatrix}$$
Where $X \in \mathbb{R}^{n-1}$, $B \in \mathrm{GL}(n-1, \mathbb{R})$, and the 0 being the zero vector in $\mathbb{R}^{n-1}$. We see the multiplication happens as
$$\begin{pmatrix} 1 & X^T \\ 0 & B \end{pmatrix}\begin{pmatrix} 1 & Y^T \\ 0 & C \end{pmatrix} = \begin{pmatrix} 1 & (Y + C^TX)^T \\ 0 & BC \end{pmatrix}$$
Since $Y^T + X^TC = (Y + C^TX)^T$. Inversion happens as
$$A^{-1} = \begin{pmatrix} 1 & -((B^{-1})^TX)^T \\ 0 & B^{-1} \end{pmatrix}$$
Meaning that this is a subgroup of $\mathrm{GL}(n, \mathbb{R})$; owing to the multiplication, we can conclude that this subgroup is isomorphic to $\mathbb{R}^{n-1} \rtimes \mathrm{GL}(n-1, \mathbb{R})$.
(As a note, it might seem as though this example has a 'backwards' multiplication: instead of our usual $h_1\varphi_{k_1}h_2$, we have $(\varphi_{k_2}h_1)h_2$. This is because the action of $\mathrm{GL}(n-1, \mathbb{R})$ on $\mathbb{R}^{n-1}$

in the question is a *right* action, wherein the matrix multiplication happens in the opposite order we're used to: $C.(X^T) = (X^T C)$, which is well defined because X^T is a $1 \times (n-1)$ matrix, and C is an $(n-1) \times (n-1)$ matrix. As an exercise, show that a right group action defined as $X \times G \to X$, $(x, g) \mapsto x.g$ is consistent with all of our previous deductions)

(3) Let H be any group, and let $K = \mathrm{Aut}(H)$. Then using $\varphi : K \to \mathrm{Aut}(H)$ just the identity map, and we can form $G = H \rtimes \mathrm{Aut}(H)$, which is called the *holomorph* of H, usually denoted $\mathrm{Hol}(H)$. For example, if $H = \mathbb{Z}_4$, then $\mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$, since there are only two generators of $\mathbb{Z}_4$. Hence, the only nontrivial automorphism of $\mathbb{Z}_4$ is the one which sends 1 to 3. Thus the holomorph of $\mathbb{Z}_4$ is $\mathbb{Z}_4 \rtimes \mathbb{Z}_2$. We see, then, that $(1,0)(0,1) = (1,1)$, and $(0,1)(1,0) = (3,1) = (1,0)^{-1}(0,1)$. One can conclude (with a little work) that $\mathrm{Hol}(\mathbb{Z}_4) \cong D_4$.

(4) Let $H = \mathrm{SL}(n, \mathbb{R})$, and let $K = \mathbb{Z}_2$ (since $\mathrm{SL}(n, \mathbb{R})$ is not abelian, this doesn't fit into example 1). Consider the map $\varphi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathrm{SL}(n, \mathbb{R}))$ where the nontrivial automorphism of $\mathrm{SL}(n, \mathbb{R})$ coming from $1 \in \mathbb{Z}_2$ is $\varphi_1(A) = (A^T)^{-1}$. Hence, we can form $G = \mathrm{SL}(n, \mathbb{R}) \rtimes_\varphi \mathbb{Z}_2$, with the more complicated multiplication example given by:

$$(A, 1)(B, 0) = (A(B^T)^{-1}, 1)$$

References

[1] David Dummit and Richard Foote, *Abstract Algebra*, 3rd ed. Wiley, **2004**

[2] John B. Fraleigh, *A Course in Abstract Algebra*, 7th ed. Pearson, **2002**

[3] Joseph Gallian, *Contemporary Abstract Algebra*, 8th ed. Cengage, **2012**