MAT347: Groups, Rings & Fields

Rishibh Prakash

September 2022

Contents

1 Groups

Groups are incredibly important objects in mathematics. Despite (or maybe because of) their simple definition, groups are quite powerful.

At their core, groups are about symmetry. Consider, for example, an equilateral triangle. The symmetries of a shape are the set of rigid motions that result in the same shape in the same position. For a triangle, we can rotate it $\frac{2\pi}{3}$ radians (counter-clockwise, say) or $\frac{4\pi}{3}$ radians. In addition, we can also reflect the triangle across the perpendicular bisector of any edge. Finally, we have the identity transformation that does nothing and leaves the triangle as it is. Thus we have a total of 6 symmetries which is also the number of ways arranging the 3 vertices allowing us to conclude that we have found all the symmetries.

Suppose ρ is the rotation by $\frac{2\pi}{3}$ and σ is the reflection that swaps vertices B and C. Then $\rho\sigma$ is the reflection that swaps and A and C while $\sigma\rho$ is the reflection that swaps A and B. It should make sense that the composition of two symmetries is itself a symmetry. Performing the first action results in the same equilateral triangle so we can perform the second action which also gives the same triangle. Thus their composition is a symmetry. Importantly, however, the order in which the composition is performed is important. In the above example, we say that σ and ρ do not commute.

A similar example are the symmetries of a square. In this case, there is the identity transformation, along with 3 rotations and 4 reflections (8 in total). Note that there are in some sense 2 kinds of reflections: those with the line of reflection through the diagonal and those with the line of reflection through the edges. The first kind of reflection fixes two of the vertices while the second kind has no fixed points. One other thing to note about all the symmetries is that they can be undone to return to the original position.

Definition 1.1 (Group)**.** A group is a set G with a composition

$$\begin{aligned} G \times G &\to G \\ (g, h) &\mapsto gh = g \circ h \end{aligned}$$

satisfying:

1. associativity: $(gh)k = g(hk)$
2. existence of identity element: $\exists e \in G$ such that $ge = eg = g$ for all $g \in G$
3. existence of inverses: for every $g \in G$, there exists some $g^{-1} \in G$ such that $gg^{-1} = e = g^{-1}g$.

Some more examples of groups are:

- $\mathbb{Z}$ (or any field) with $+$ as the operation
- $\mathbb{Z}/n\mathbb{Z}$ with addition mod n
- $SL(n, \mathbb{F})$ which is the set of all $n \times n$ matrices over a field $\mathbb{F}$ with determinant 1

2 Examples of Groups

2.1 Fields

A field $\mathbb{F}$ consists of 2 (commutative) groups. First we have the additive group $(\mathbb{F}, +)$ with 0 as the identity and for every $x \in \mathbb{F}$ we have its 'inverse' as $-x$. We also have the multiplicative group, often denoted $\mathbb{F}^\times$, which consists of the non-zero elements of $\mathbb{F}$ with the operation of (surprise, surprise) multiplication. In this case the identity is 1 and the inverses are the usual multiplicative inverses.

Given a field, we can also construct a number of related matrix groups.

- General linear group, $GL(n, \mathbb{F})$ = set of invertible $n \times n$ matrices (with entries in $\mathbb{F}$)
- Special linear group, $SL(n, \mathbb{F})$ = set of matrices with determinant 1
- Special orthogonal group, $SO(n)$ = set of matrices A in $SL(n, \mathbb{F})$ such that $AA^T = I$. If $\mathbb{F} = \mathbb{R}$, then this is the set of rotations in $\mathbb{R}^n$.

Meandering Questions 2.1. The cardinality of a group G is also called its order and is typically denoted $|G|$. If $\mathbb{F}$ has finite order, what is the order of the above matrix groups?

2.2 Cyclic groups

Another important example of a group is $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$. You typically think of this group as consisting of elements $\{0, 1, \ldots, n-1\}$ with the operation being addition mod n. To remind us that we are working with modular arithmetic, we often but a bar on top of the numbers, e.g. if $n = 8$, we might write $\overline{5} + \overline{7} = \overline{4}$. As one might expect, the identity is $\overline{0}$. Note that in this group $\overline{k}^{-1} = \overline{-k} = \overline{n-k}$.

There is a very natural correspondence between $\mathbb{Z}/n\mathbb{Z}$ and the n-th roots of unity. In particular, we can map $\overline{k}$ to $e^{\frac{k \cdot 2\pi i}{n}}$. The cyclic structure of the group is made particularly clear in the latter case (consider what $\overline{k+n}$ is mapped to) motivating the name *cyclic group* for $\mathbb{Z}/n\mathbb{Z}$. In general, the cyclic group of order n is denoted C_n.

2.3 Quaternion group

The quaternion group $\mathbb{H}$ is a group of 8 elements

$$\mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}$$

with the multiplication defined as follows

$$\begin{aligned} ij &= -ji = k \\ jk &= -kj = i \\ ki &= -ik = j \\ i^2 = j^2 &= k^2 = -1 \end{aligned}$$

The 1 is (of course) the identity and multiplication with -1 switches signs as you would expect.

Remark 2.1. Sometimes, $\mathbb{H}$ is also used to refer to the set of all linear combinations of i, j, k. This is often called the set of all quaternions or the Hamiltonian algebra.

3 Subgroups

Consider the triangle group from the previous section and consider just the rotations (including the identity element, which you can think of as a rotation by 0). It is easy to see that this set forms a group in its own right and in fact is (isomorphic to) the cyclic group of order 3.

Definition 3.1 (Subgroup)**.** A non-empty subset H of a group G is a subgroup, denoted $H \leq G$, if H is a group using the same operation as G. In other words, for all $h, k \in H$ we have $hk \in H$ and $h^{-1} \in H$.

Remark 3.2. The conditions automatically imply that $e \in H$.

Remark 3.3. If $\mathbb{F}$ is a field then we know that $(\mathbb{F}, +)$ is a group and $\mathbb{F}^\times$ is a subset of $\mathbb{F}$. But it is not a subgroup since the operations are different.

Proposition 3.4 *If $H \subset G$ is non-empty, then $H \leq G$ if and only if $hk^{-1} \in H$ for all $h, k \in H$.*

Proof. Exercise (cute) □

Consider the powers of i in $\mathbb{H}$. Since $i^2 = -1, i^3 = -i$ and $i^4 = 1$, we see that $\{1, i, -1, -i\}$ forms a (cyclic) subgroup of $\mathbb{H}$. We say that this (sub)group is generated by i and denote it $\langle i \rangle$. In general, given a group G and $g_1, \ldots, g_n \in G$, we use $\langle g_1, \ldots, g_n \rangle$ to denote the smallest subgroup of G that contains $g_1, \ldots, g_n$. The generator of a subgroup need not be unique. Looking at the above example of the subgroup of $\mathbb{H}$, we see that it is also generated by $-i$.

Suppose we are given $g \in G$ such that there exists some $m \in \mathbb{N}$ satisfying $g^m = e$. Let $n = \min\{m \in \mathbb{N} : g^n = e\}$. Then $|\langle g \rangle| = n$. We also say that the order of g is n (this is the order of an element of a group rather than the order of a group). If no such m exists, then the order of g is infinite and $\langle g \rangle = \{1, g^{\pm 1}, g^{\pm 2}, \ldots\}$ is isomorphic to $\mathbb{Z}$.

4 Cosets

As is so typical in mathematics, we begin with a definition.

Definition 4.1 ((Right) cosets)**.** Let G be a group and $H \leq G$ is a subgroup. Take some $g \in G$ and consider

$$Hg := \{hg : h \in H\}$$

This is called a *(right) coset* of H.

Remark 4.2. One can equivalently define left cosets by considering gH instead.

The remarkable thing about cosets is that they are either disjoint or equal. Let us prove this statement.

Proposition 4.3 *Let $g, g' \in G$. Then Hg and Hg' are either disjoint or equal.*

Proof. Suppose Hg and Hg' are not disjoint. Thus there lies something in the intersection. This means that

$$hg = h'g'$$

for some $h, h' \in H$. Then $g = h^{-1}h'g'$. Since H is a subgroup, $h^{-1}h' \in H$ implying that $g \in Hg'$. Similarly we can conclude that $g' \in Hg$.

Now consider an arbitrary element in Hg, call it kg where $k \in H$. Then

$$kg = kh^{-1}h'g'$$

is also an element of Hg' since $kh^{-1}h' \in H$. Therefore $Hg \subset Hg'$ and symmetrically we can conclude that $Hg' \subset Hg$ giving us the final conclusion $Hg = Hg'$. □

This means that (right) cosets of H partition G (one needs to show that the union of all the cosets is indeed G but this is clear since for every $g \in G$, we can find g in Hg).

Additionally, note that if $hg = h'g$ then $h = h'$ (we multiply by g^{-1} on the right on both sides). Hence each $h \in H$ gives a difference element hg in Hg. This means that

$$|Hg| = |H|$$

Thus we find that

$$|G| = (\#\text{ of distinct cosets}) \cdot |H|$$

We have just proven Lagrange's theorem.

Theorem 4.4 (Lagrange's Theorem) *If $|G| < \infty$ and $H \leq G$ then $|H|$ divides $|G|$.*

We often write $\frac{|G|}{|H|} = [G : H]$ and called it the *index* of H in G. Thus we could equivalently write

$$|G| = [G : H] \cdot |H|$$

a statement which also holds for infinite groups since if $|G| = \infty$ then (at least) one of the terms on the right will be infinite.

Let us consider some consequences of Lagrange's theorem. For example let G be a group of order p where p is a prime number. Then we know that G cannot have non-trivial subgroups. In other words, the only subgroups of G are $\{e\}$ and G itself. We know a G of order p exists of course, take $\mathbb{Z}/p\mathbb{Z}$, and we will see later that this is the only group of this order.

4.1 Example

Let $G = \mathbb{Z}$ be the integers and consider $\mathbb{H} = 2\mathbb{Z}$ the even integers. Then $H + 0 = H$ (the set of all even integers) is one coset and $H + 1$ (the set of all odd integers) is the other coset. We know there can't be any more cosets since these two cover the whole group. Thus

$$\mathbb{Z} = 2\mathbb{Z} \dot{\cup} 2\mathbb{Z} + 1$$

which is to say

$$[\mathbb{Z} : 2\mathbb{Z}] = 2$$

4.2 Interaction of cosets

Everything so far also holds for left cosets, by flipping the order and words when necessary. The more interesting thing to consider is the interaction between left and right cosets.

Consider for example the triangle group we have been working with so far. We have the three rotations e, ρ, ρ^2 and the reflections $\sigma_A, \sigma_B, \sigma_C$ where σ_K is the reflection that fixes vertex K. Therefore $G = \{e, \rho, \rho^2, \sigma_A, \sigma_B, \sigma_C\}$. We will take our subgroup to be $H = \{e, \sigma_A\}$. Then the right cosets are

$$\begin{aligned} He &= H = \{e, \sigma_A\} \\ H\rho &= \{\rho, \sigma_A\rho\} = \{\rho, \sigma_B\} \\ H\rho^2 &= \{\rho^2, \sigma_A\rho^2\} = \{\rho^2, \sigma_C\} \end{aligned}$$

On the other hand left cosets are

$$\begin{aligned} eH &= H = \{e, \sigma_A\} \\ \rho H &= \{\rho, \rho\sigma_A\} = \{\rho, \sigma_C\} \\ \rho^2 H &= \{\rho^2, \rho^2\sigma_A\} = \{\rho^2, \sigma_B\} \end{aligned}$$

Note how different these are. The right coset containing ρ contains σ_B while the left coset containing ρ contains σ_C. This illustrates that in general, left and right cosets can be completely different. The exception of course is if G is commutative since in that case the order of multiplication does not matter. The one that remains constant, regardless of whether or not G is commutative, is the number of cosets.

5 Action

Definition 5.1 (Group action)**.** An action of a group on a set X is a map

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto g \cdot x = gx \end{aligned}$$

such that for any $x \in X$ we have

1. $e \cdot x = x$
2. $(gh) \cdot x = g(h \cdot x)$

5.1 Groups acting on themselves

If G is a group, then it can act on itself. The most obvious manner of defining $g \cdot x$ is to use the group operation itself so that $(g, x) \mapsto gx$. This is called *left translation* or the *left regular action*.

One might wonder whether we could define (g, x) to map to xg. In this case note that (gh, x) maps to xgh where $(g, (h, x))$ is sent to xhg. Since in general $hg \neq gh$, we see that this is not action. However we can 'fix' this by using the inverse. Namely the map $(g, x) \mapsto xg^{-1}$ is indeed an action. This is what we call a *right translation* or *right regular action*. Finally we have conjugation which can be thought of as a combination of the previous two actions and is arguably the most important one. In this case, we have $(g, x) \mapsto gxg^{-1}$.

5.2 Example

Let G be $SO(3) = \{A \in \mathbb{R}^{3\times 3} : \det(A) = 1 \text{ and } AA^T = I\}$. This is of course the set of all rotations in $\mathbb{R}^3$. It is easy to see that G acts on S^2 exactly by rotating it. Note we can embed $SO(2)$ in $SO(3)$ by fixing the z-axis. To be precise, we define

$$H := \left\{ \begin{pmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} : \theta \in [0, 2\pi) \right\}$$

We see that H only rotates the $x - y$ plane thus it maps a point to some other point at the same altitude (fixing the north and south poles).

5.3 Orbits

Definition 5.2. If G acts on X and $x \in X$ the the *orbit* of x (under G) is the set of all points x take to by elements of G and is often denoted

$$G \cdot x := \{gx : g \in G\}$$

Remark 5.3. The orbits of H on the sphere are the lines of latitude and the north and south poles.

We see that given a pair of points on the sphere there is a rotation that takes the first point to the second point. Thus Gx for any $x \in S^2$ is simply S^2 again.

Let us instead consider H then. The orbit of N, the north pole, under H is simply $\{N\}$. This means that for any $g \in G$, we have $gHN = gN$ since $ghN = gN$ for every $h \in H$. Thus every element of gH maps N to the same point or in other words, every coset maps N to a unique point. We may wonder whether this mapping is 1-1. In other words, can two different cosets maps N to the same point. Suppose this is the case. In other words, we have $gHN = g'HN$ which is to say $gN = g'N$. Recall that N is an element of the set S^2 and not the group. So we cannot conclude that $g = g'$. On the other hand what we do have is that $g^{-1}g'N = N$. Since $g^{-1}g'$ fixes N it must be an element of H (we have not shown that H contains all elements that fix N but hopefully this is easy to see intuitively). But if $g^{-1}g' \in H$ then $gH = g'H$. Thus not only do individual cosets map N to a single point, distinct cosets map N to distinct points. Since we know that N can be mapped to any point on the sphere by choosing an appropriate g we conclude that points on the sphere are in 1-1 correspondence with the (left) cosets of H.

6 Stabilizers and Centralizers