Lecture 2 — Subgroups

Dr. D. Bernhard

In this lecture: subgroups — generators — order of elements — Lagrange's theorem — permutations as groups — cycles

Learning outcomes: After this lecture and revision, you should:

- Understand subgroups and their possible sizes and be able to apply this knowledge to compute them in any finite group.
- Be able to check whether or not a subset of a group is a subgroup, and extend a subset to the smallest subgroup that contains it if not.
- Understand the order of elements in a group and be able to compute the possible orders of elements of a finite group and find an element of a given order (in particular a generator) if one exists.
- Understand the structure of the set S of permutations on a set A as a group and be able to compose and invert permutations.
- Be able to decompose permutations into disjoint cycles, compose cycles and compute permutations from cycles.

2 Subgroups

We continue our quest to understand groups and how they work. If we are given any structure $(G, +)$ and told that is a group, we already know a lot about how the $+$ operation can behave — today, we look at what happens when the same $+$ operation is used on subsets of G and we look at another way to get examples of groups, namely permutations.

2.1 Opening example

Start with the group $\mathbb{G} = (\mathbb{Z}_{32}, +_{32})$. If we pick a subset H of the set $\mathbb{Z}_{32}$ with the same operation, do we get a group? Here's a table of elements:

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31

Let's try the first column $H = \{0, 8, 16, 24\}$. The group operation on these elements has the table

$+_{32}$	0	8	16	24
0	0	8	16	24
8	8	16	24	0
16	16	24	0	8
24	24	0	8	16

This is a group operation, so $(H, +_{32})$ is a group. But if we tried the subset $H' = \{0, 1, 2, 3, 4, 5, 6, 7\}$, we would not get a group: $6 +_{32} 6 = 12$ which is not in H' anymore, for example.

2.2 Definition of a subgroup

> **Definition 2.1.** Let $\mathbb{G} = (G, +)$ be any group. Let H be a subset of G. If $\mathbb{H} = (H, +)$ is a group for the same operation $+$, we say that $\mathbb{H}$ is a subgroup of $\mathbb{G}$.

When we defined groups, we defined $+$ to be an operation $G \times G \to G$ so by definition, adding two group elements produced another group element. If we take a subset H but the same operation, even if we add two elements of H we have no guarantee that we will end up in H again. So what the definition of subgroups is really about is that doing group operations on H-elements lands in H again. To check that something is a subgroup we do not need to check that the operation is associative etc. — we already know this because it is a group operation. Instead, we have three new rules:

> **Proposition 2.2.** If $(G, +)$ is a group and H is a subset of G then $(H, +)$ is a subgroup of G if and only if the following three conditions hold.
>
> 1. The neutral element e is in H.
> 2. For any two elements a, b in H their sum $a + b$ is also in H.
> 3. For any element a in H, its inverse $(-a)$ is also in H.

Another way of stating this is saying that a subgroup is formed by a subset that is closed under the group operation (using the group operation you cannot "escape").

Let's take the group $(\mathbb{Z}, +)$ and the subset $H = \{0, 1, \ldots, n-1\}$ for some $n > 0$. Using the same operation $+$, we see that 1 and $n-1$ are both elements of H but $1 + (n-1) = n$ which is not an element of H. So H cannot be a subgroup. This brings us to a

WARNING: $(\mathbb{Z}_n, +)$ is NOT a subgroup of $(\mathbb{Z}, +)$!

The two groups have different $+$ operations. As in the last lecture, we could write $+$ and $+_n$ to make this clear.

Something that is a subgroup of $(\mathbb{Z}, +)$ is the subset of even numbers with the usual addition, as can be seen by checking the three conditions above: 0 is even, the sum of two even numbers is even and the inverse of an even number is even. the same holds for multiples of any number: for $n \in \mathbb{N}$, the subset

$$n\mathbb{Z} := \{n \cdot z \mid z \in \mathbb{Z}\}$$

forms a subgroup of $\mathbb{Z}$ with addition. Note that $\mathbb{Z} = 1\mathbb{Z}$ and $0\mathbb{Z} = \{0\}$ which is a subgroup with one element. More generally, every group $(G, +)$ has two trivial subgroups:

Definition 2.3. The two trivial subgroups of a group $(G, +)$ are $(G, +)$ itself and $(\{e\}, +)$ where e is the neutral element. All other subgroups are called non-trivial subgroups.

2.3 Generators

How do we find subgroups of a group? The example with the even numbers $2\mathbb{Z}$ in $\mathbb{Z}$ suggests that we can try the following: for a given group $\mathbb{G} = (G, +)$, pick any element g and look at the "multiples" $g, g+g, g+g+g, \ldots$. Actually we have to add the neutral element e and the inverses $(-g), (-g) + (-g), \ldots$ too if we want to end up with a group.

Definition 2.4 (subgroup generated by element). Let $(G, +)$ be a group and g any element of G. The subgroup generated by g, written $\langle g \rangle$, is the group containing exactly the following elements:

- g is an element of $\langle g \rangle$.
- The neutral element e is an element of $\langle g \rangle$.
- If a, b are elements of $\langle g \rangle$ then so is $a + b$.
- If a is an element of $\langle g \rangle$ then so is $(-a)$.

The way we wrote this definition automatically makes it into a subgroup. As an example, for any integer z we have $\langle z \rangle = z\mathbb{Z}$ in the group $\mathbb{Z}$, i.e. $\langle 2 \rangle$ really is the subgroup containing exactly the multiples of 2. In any group, the neutral element generates a subgroup with only one element — itself: $\langle e \rangle = (\{e\}, +)$.

In $\mathbb{Z}$, there happens to be an element 1 with the property that $\langle 1 \rangle = \mathbb{Z}$, i.e. 1 generates the whole group. We call such elements, if they exist, generators:

> **Definition 2.5 (generator, cyclic group).** Elements g of G in a group $(G, +)$ with $\langle g \rangle = G$ are called generators. If a group has a generator, it is called a cyclic group.

Not all groups have generators but we will have to wait a bit to see an example of a group that does not have one.

Exercise. $(\star)$ $\mathbb{Z}$ has one other generator besides 1; which?

The definition of generating a subgroup by one element generalises to several elements.

> **Definition 2.6 (subgroup generated by multiple elements).** Let $(G, +)$ be a group and $g_1, \ldots g_n$ be elements of G. The subgroup $\langle g_1, \ldots, g_n \rangle$ is the subgroup containing exactly the following elements:
>
> - $g_1, \ldots, g_n$ are all elements of $\langle g_1, \ldots, g_n \rangle$.
> - The neutral element e is an element of $\langle g_1, \ldots, g_n \rangle$.
> - If a, b are two elements of $\langle g_1, \ldots, g_n \rangle$ then so is their sum $a + b$.
> - If a is an element of $\langle g_1, \ldots, g_n \rangle$ then so is $(-a)$.
>
> If $\langle g_1, \ldots, g_n \rangle = G$ then we say that G is generated by the elements $g_1, \ldots, g_n$.

The group $\langle g_1, \ldots, g_n \rangle$ is the smallest subgroup of G that contains the elements $g_1, \ldots, g_n$. Every group is generated by some set of elements: one can always take all of them to get $\langle G \rangle = G$. Whether an infinite group is generated by a finite subset of its elements is a more interesting question, but one that we will not investigate any further here.

2.4 Order of elements and Lagrange's theorem

We can define the order of an element by looking at the subgroup that it generates:

Definition 2.7 (order of an element). The order of an element g in a group $\mathbb{G} = (G, +)$ is the order of the subgroup $\langle g \rangle$.

We can predict what the orders of elements in a finite group can be. In fact, if we know that any $\mathbb{H}$ is a subgroup of $\mathbb{G}$ then we know a lot about what $\mathbb{H}$ can look like. One of the most important facts if $\mathbb{G}$ is finite is Lagrange's theorem:

Theorem 2.8 (Lagrange). If $\mathbb{G} = (G, +)$ is a finite group then the order of any subgroup of $\mathbb{G}$ divides the order of $\mathbb{G}$.

In our opening example, we found a subgroup H of 4 elements in $(Z_{32}, +)$ and indeed, 4 divides 32. Actually, H was the subgroup $\langle 8 \rangle$. We will not prove Lagrange's theorem here but a proof can be found at the end of these notes.

If $\mathbb{G}$ is finite, Lagrange's theorem tells us that the order of each element must divide the order of $\mathbb{G}$. For example in $(\mathbb{Z}_6, +)$, the only possible orders of elements are $1, 2, 3$ and 6. Elements of order 6, the same as the order of the whole group, are exactly the generators.

Exercise. *Small orders and small groups.*

1. ($\star$) Find the orders of all elements in the groups $(\mathbb{Z}_4, +_4)$, $(\mathbb{Z}_5, +_5)$ and $(\mathbb{Z}_6, +_6)$.
2. ($\star\star$) In any group, the only element of order 1 is the neutral element. Why?
3. ($\star\star$) A prime number p is a natural number greater than 1 whose only divisors are 1 and p. What can you say about the order of elements in $(\mathbb{Z}_p, +_p)$ when p is prime? (Look at $(\mathbb{Z}_5, +_5)$ again for a hint; compute all orders in $(\mathbb{Z}_7, +_7)$ if you need an extra hint since both 5 and 7 are prime.)

Exercise. ($\star\star$) *The L block.* An L block consists of four squares arranged in the shape of the letter capital L. Suppose we have an L block and two operations A and B that rotate it by 90 degrees clockwise and anticlockwise respectively as in Figure 1.

We can describe these actions on the L block by a group. Its elements are the possible rotations of the L block starting in the upright position. We can describe each operation by a (possibly empty) sequence using the letters A and B as shown in the diagram.

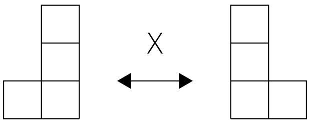
Two sequences of letters may describe the same operation, such as $ABABA$ and BBB. So let's introduce an equivalence relation: two sequences are equivalent if they produce the same rotation of the L block.

1. Describe a sensible set of representatives for these equivalence classes (hint: take the alphabetically first, shortest sequence from each class).

2. Give the rules to compute the representative element $[s]$ given a sequence s. (Hint: the rules will say that you can cancel certain subsequences.) Find the representatives of AAA, $ABABA$, $AAAA$ and $BBBBA$ using these rules.

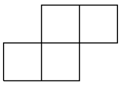
3. Label the representative elements with the numbers $0, 1, 2, 3$ in such a way that composing sequences matches addition in $\mathbb{Z}_4$. For example, if some sequence s gets the label 1 and t gets 2, then representative of the composition st should get the label $3 = 1 + 2$.

4. Suppose we added an extra move X that "mirrors" the L block horizontally:

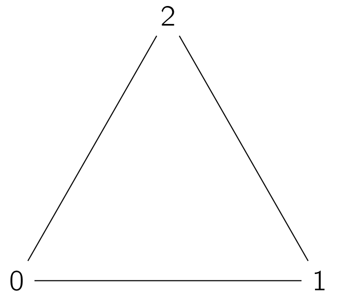


Redo the construction of a group of operations from before. How many elements do you end up with? Find sensible representatives. Why can you not label these elements with numbers $0, 1, \ldots, n-1$ anymore in such a way that addition of labels in $(\mathbb{Z}_n, +)$ matches composing transformations?

5. If you redo the same construction (with the X operation) for the S block (below), you get a group with four elements. Find a way to represent elements of this group as 2-bit numbers such that the group operation becomes the exclusive or (XOR) operation.



Note: in addition to L and S blocks, the same construction can be done with any regular n-gon where the vertices are labelled with the numbers $0, 1, \ldots, n-1$. Here is the regular 3-gon, a.k.a. triangle:



The group of rotations of such a n-gon around its centre, where two rotations are equivalent if they place all labels in the same place, is called the n-th cyclic group C_n and is another way or writing $(\mathbb{Z}_n, +)$ (for example by tracking the position of the 0 label). If we add the "mirroring" operation, we get a non-Abelian group of $2n$ elements called D_n. C_n is a subgroup of D_n and both are subgroups of S_n, the group of all permutations of the labels 0 through $n-1$.

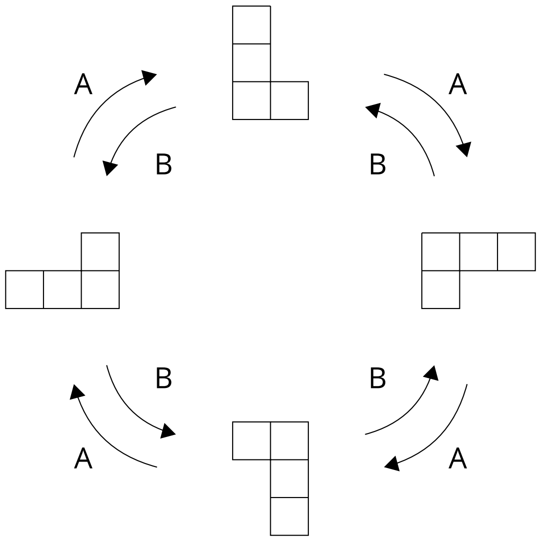


Figure 1: The L block (see exercises).

Exercise. *Free groups.* Here is another way to construct groups, similar to the idea with the L block and sequences of operations above. Pick any finite alphabet $\{A, B, C, \ldots\}$ of letters. For each letter, add an anti-letter which we denote by $\{\bar{A}, \bar{B}, \bar{C}, \ldots\}$ (none of the original letters is allowed to be the same as any of the anti-letters).

Our group elements are sequences (including the empty one) of letters and anti-letters where no letter is allowed to stand next to its anti-letter. The group operation $s + t$ on two sequences s, t is done by writing the sequence s followed by t, then repeatedly cancelling any pairs of a letter with its anti-letter. For n letters, this is called the free group on n generators.

1. ($\star$) What is the neutral element? How do you compute the inverse of a sequence?
2. ($\star\star$) Convince yourself informally that this is a group (a full proof is not required!)
3. ($\star$) Convince yourself that the set of original letters really is a set of generators for this group.
4. ($\star$) For the free group on two generators A, B, find two elements (words) v, w such that $v + w \neq w + v$.
5. ($\star\star$) The free group on one generator is just another way of describing $(\mathbb{Z}, +)$. Explain how you could label sequences with integers such that the sum of two sequences is labelled by the sum of their labels.

Exercise. ($\star\star\star$) *Free groups via equivalence relations.* This is the "official" way to define free groups (and prove that they are groups):

- Take the set of all words containing the letters or their anti-letters (including the empty word) with no restrictions.
- Define an equivalence relation $\sim$ under which two words are equivalent if one can be obtained from the other by adding or removing pairs of a letter followed by its anti-letter (or the other way round).
- Take the set of equivalence classes of all words under $\sim$. Each class contains exactly one word that has no pairs of a letter and its anti-letter; take this word as the representative of the class.

Check that the relation $\sim$ described here really is an equivalence relation and that every equivalence class contains a word that has no pairs of a letter next to its anti-letter. (You don't need to prove that each class contains only one such word.)

The following sections are not presented in the lectures but are intended for self-study.

2.5 Permutation groups

Besides groups derived from $\mathbb{Z}$ there are many other ways to construct groups. Permutations are another example of a structure that produces groups.

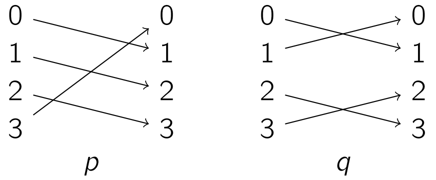
> **Definition 2.9 (permutation).** A permutation on a finite set S of elements is a bijective map p from S to itself. If the elements of S are $s_1, \dots, s_n$ then a permutation p can be written in the form
>
> $$\begin{pmatrix} s_1 & s_2 & \dots & s_n \\ p(s_1) & p(s_2) & \dots & p(s_n) \end{pmatrix}$$

In the rest of this lecture we will use $\{0, 1, \dots, n-1\}$ as an example set of size n. Indeed, to define permutations it makes no difference which set of a given size we pick — the elements are just "labels" for the permutations to work on.

We can also draw permutations as diagrams. For example, here are two permutations on the set $S = \{0, 1, 2, 3\}$:

$$p = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix} \quad q = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

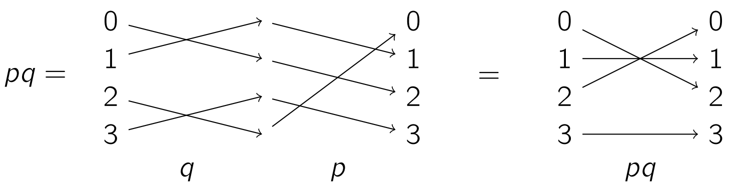
As diagrams, the permutations look like this:



What makes permutations into a group is the fact that they can be composed. This is easiest to see if we take two permutation diagrams and glue the arrows together in the middle. Unfortunately, there are two different ways we can do this and while our way is perhaps the more common, both ways can be found in different textbooks. For us, composing p and q means that we write the diagram of q on the left and that of p on the right, then glue the arrows together.

We also need a name for this operation. We choose the more standard pq (rather than $p + q$). The choice of symbol to mean "compose", unlike the order in which we compose things, is just a matter of notation and does not change what we are doing.

At the moment it might look "backwards" to use pq to mean the object you get when you compose with q on the left. We will explain this in a moment but first let's look at an example with the permutations p and q from above. We compose two permutation diagrams by glueing the arrows together in the middle:



This gives us the permutation

$$pq = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 1 & 0 & 3 \end{pmatrix}$$

WARNING. The order in which one writes a composed permutation varies from textbook to textbook. We call this object pq. Some authors would call it qp instead. As we will see in a moment, this is important: $pq \neq qp$.

The reason that we take pq to mean "q glued to p" and not the other way round is that permutations are formally functions on a set of elements: for the permutations p and q in the example, we could try and evaluate $p(q(0))$. Since $q(0) = 1$, this becomes $p(1)$ which is 2. In other words, to calculate $p(q(0))$ we apply q first, then p. This is actually the formal definition of our way of composing permutations:

Definition 2.10 (composition of permutations). For two permutations p and q on the same set X, their composition pq is the permutation such that for all $x \in X$ we have $pq(x) = p(q(x))$.

Whichever way round we define composition, we get a group:

Definition 2.11 (symmetric group). For any positive integer n, the symmetric group S_n is the group whose elements are the permutations of the set $\{0, 1, \ldots, n-1\}$ and the group operation is composition.

Let's check that this is actually a group (this is not a full proof). For associativity, look at the diagrams of any three permutations: it does not matter which two you glue together first as long as you keep the three diagrams in the same order. The neutral element is the permutation that maps every element to itself, sometimes written id (for "identity"). The inverse of a permutation can be found by reversing all arrows in the diagram and taking the mirror image.

Of course, one can define the group of permutations over any set S. But the structure of this group depends only on the number of elements that S has, so for finite sets S one can consider only the sets $\{0, 1, \ldots, n-1\}$ "without loss of generality". What we are actually doing is taking this set as representative element of the "class of all sets with n elements".

Permutation groups are an example of non-commutative groups. (Easy exercise: find qp for the p, q given above and check that $pq \neq qp$.)

2.6 Subgroups of permutation groups

Take the group S_n of permutations on any set A of n elements (the set $\{0, 1, \ldots, n-1\}$ will do fine). Pick any subset B of A and consider only the permutations S' that leave all elements outside B alone. For example, if $A = \{0, 1, 2, 3\}$ and $B = \{0, 1, 2\}$ then the permutation

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 2 & 1 & 3 \end{pmatrix}$$

leaves the elements outside B alone — the only such element is 3. (It is irrelevant for S' whether or not the permutation leaves anything inside B alone.) It turns out that S' is a subgroup of S_n. The neutral element id of S_n leaves every element alone so it certainly leaves those outside B alone; if two permutations both leave some element alone then so does their composition — as can be seen on their diagrams, the composition of two horizontal lines is still a horisontal line. The same argument on diagrams shows that if some permutation p leaves an element x alone then so does its inverse: reversing a horizontal arrow gives another horizontal arrow. We have informally shown the following:

> **Proposition 2.12.** For any positive integers $m \leq n$, the group S_m is a subgroup of S_n.

2.7 Cycles

Another way to look at permutations is to consider cycles.

> **Definition 2.13.** On a set A, a cycle of length k is a list of elements of A with no repetitions $(a_1, a_2, \ldots, a_k)$. The empty cycle (of length 0) is written $()$.

A cycle defines a permutation by sending a_1 to a_2 etc., and a_k back to a_1. For example, on the set $A = \{0, 1, 2, 3, 4, 5, 6, 7\}$ the cycle $(5, 1, 2)$ defines the permutation

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 2 & 5 & 3 & 4 & 1 & 6 & 7 \end{pmatrix}$$

The empty cycle () gives the identity permutation id. For any cycle or set of cycles c, we can look at the group $\langle c \rangle$ that they generate. This is by definition a subgroup of S_n.

The notation for cycles does not uniquely describe a permuation: $(5, 1, 2)$ and $(1, 2, 5)$ both give the same permutation. (Exercise: there is one other way to write the same permutation as a cycle, which one?) However $(5, 2, 1)$ describes a different permutation.

The interesting thing about cycles is that they can be used to build all permutations.

Proposition 2.14. Any permutation $p \in S_n$ can be written as a composition of cycles with disjoint elements. If we take the underlying set to be $\{0, \dots, n-1\}$ then there is an ordering under which each permutation has exactly one normal form as a composition of disjoint cycles:

- Shorter cycles come before longer ones.
- For two cycles of the same length, the one with the smallest element comes first.
- Within each cycle, the smallest element is the first.

There are several useful rules for computing with cycles which we will use to prove this proposition. The composition of two cycles is the composition of their permutations (in the same order as the cycles are given), so the expression $(0, 1)(2, 3)$ on the set $\{0, 1, 2, 3\}$ is the composition

$$(0,1)(2,3) = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 2 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

1. If you rotate the elements in a cycle around by taking the last element and placing it as the new first element, you get the same permutation. Conversely, two cycles describe the same permutation if and only if one can be rotated to give the other.

   For example, $(1, 2, 3)$ and $(3, 1, 2)$ both describe the same permutation.

2. If c and d are two disjoint cycles (they do not share any elements) then $cd = dc$.

   In the example above, one can check that $(1, 0)(2, 3) = (2, 3)(1, 0)$.

3. If two cycles c, d share exactly one element x, their composition is the cycle obtained by rotating x to be in the last place of c and the first place of d, and "glueing together" the x-es, dropping the middle parentheses.

   For example, to compute $(1, 2, 3)(2, 4)$ we write this as $(3, 1, 2)(2, 4)$ and glue the 2-s to get $(3, 1, 2, 4)$.

Rules 1 and 2 together say that if we have any way of representing a permutation as a composition of disjoint cycles then we can reorder the cycles and the elements within cycles to get the unique representation from proposition 2.14.

As an example, consider the set $A = \mathbb{Z}_8$ and the permutation

$$p = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 0 & 1 & 6 & 5 & 7 \end{pmatrix}$$

Starting with 0, we find $p(0) = 3$ and $p(3) = 0$ so we have our first cycle $(0, 3)$. As we move through the elements we get the other cycles $(1, 2, 4)$ and $(5, 6)$, which we can order to write

$$p = (0, 3)(5, 6)(1, 2, 4)$$

Exercise. *Permutations — the case $n = 3$.*

1. $(\star)$ Write out all permutations on the set of three elements $\{0, 1, 2\}$.
2. $(\star)$ Find two elements p, q of S_3 such that $pq \neq qp$.
3. $(\star)$ Decompose all the elements of S_3 into cycles.
4. $(\star\star)$ Write out the "addition table" (composition table) for S_3, representing the elements as cycles.
5. $(\star\star)$ You have just shown that S_3 is not commutative. Conclude that for any $n \geq 3$, S_n is not commutative either. What about S_1 and S_2?

Exercise. $(\star)$ *Permutations in general.* Consider

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \quad q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix}$$

- Compute pq and qp.
- What are the orders of p and q?
- Decompose p and q into cycles.
- Write the following as permutations: (154), (12)(54) and (1254)(4531).

2.8 $\diamond$ Cosets and a proof of Lagrange's theorem.

$\diamond$ For any group $\mathbb{G} = (G, +)$ with a subgroup $\mathbb{H} = (H, +)$ we can define an equivalence relation $\sim_H$ on G: let $g \sim_H k$ hold if and only if there is an element h of H such that $g + h = k$. $\sim_H$ is an equivalence relation because it is (i) reflexive: $g + e = g$ for any g and e is an element of H; (ii) symmetrical because if $g + h = k$ then $k + (-h) = g$ and $(-h)$ must also be in H; (iii) transitive because if $g + h = k$ and $k + h' = l$ for elements g, k, l of G and h, h' of H then $g + (h + h') = l$ and $h + h'$ must also be in H. In fact, the three conditions for H being a subgroup match exactly with the three conditions for $\sim_H$ being an equivalence relation, so we could define subgroups via equivalence relations if we wanted to.

In our opening example, the relation $\sim_H$ that we get this way is exactly the relation $\sim_8$ that we know from the last lecture; this is not a coincidence of course. What we are doing now is more general since we can build an equivalence relation out of a subgroup even if the elements of these groups are not "numbers".

Every element of G thus lands in exactly one equivalence class of $\sim_H$ and all of H lands in the same class. We claim that all equivalence classes have the same number of elements. This way, if we write $|\mathbb{G}|$ for the number of elements of G and $|\mathbb{H}|$ for the number of elements in H then $|\mathbb{G}| = |\mathbb{H}| \cdot c$ where c is the number of classes that $\sim_H$ creates, proving the theorem. This number of classes is important enough that it gets its own name:

> **Definition 2.15.** The index of $\mathbb{H}$ in $\mathbb{G}$, written $[\mathbb{G} : \mathbb{H}]$, is the number of classes that the relation $\sim_H$ creates in G.

Lagrange's theorem in a more general form actually says:

$$|\mathbb{G}| = |\mathbb{H}| \cdot [\mathbb{G} : \mathbb{H}]$$

Cosets. Another way to define these equivalence classes is via left cosets. We will use cosets to prove Lagrange's theorem.

> **Definition 2.16 (left coset).** Let $\mathbb{H} = (H, +)$ be a subgroup of $\mathbb{G} = (G, +)$. The left coset of H at an element $g \in G$ is the set
> $$g + H := \{g + h \mid h \in H\}$$

It is not hard to see that for any $g \in G$, the coset $g + H$ is exactly the equivalence class $c(g)$ under $\sim_H$. (Left as an exercise for the mathematically proficient.) What we are trying to prove is that all cosets have the same size and we can do this by giving a bijection between them: let g and k be any two elements of G. Then the function $f : x \mapsto k + (-g) + x$ is a bijective map from $g + H$ to $k + H$ with inverse $f^{-1} : x \mapsto g + (-k) + x$. To see this, pick an element of $g + H$ and write it as $g + h$ for $h \in H$ as per its definition. Then $f(g + h) = k + (-g) + g + h = k + h$ is an element of $k + H$, showing that the function maps $g + H$ into $k + H$. Further for any element x we have $f^{-1}(f(x)) = g + (-k) + k + (-g) + x = x$ and the same holds for $f(f^{-1}(x))$. So any two left cosets of H are in bijection and therefore of the same size. Since $H = e + H$ for the neutral element e, this proves Lagrange's theorem.

We close with a few comments. We could do the same argument with right cosets as well as left cosets; in an Abelian group the two are the same anyway.

Infinite groups. The whole construction of cosets and indices works equally well for infinite groups, for example for $n > 0$ we have $[\mathbb{Z} : n\mathbb{Z}] = n$. An index can also become infinite: $[\mathbb{Z} : 0\mathbb{Z}] = \infty$ since the resulting equivalence relation is just the $=$ (equals) relation so every element is its own equivalence class.

A version of Lagrange's theorem holds for infinite groups too but the reason that we did not give it here is that we would have first to define what "divides" means when infinities are involved, which is beyond what we want to cover in this course.