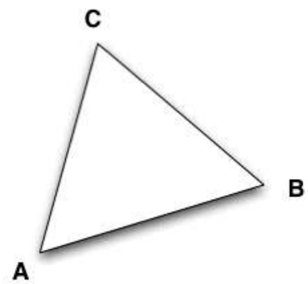
Classroom strategy: Students will work in small groups on a series of questions to understand the objectives. Transition between questions such as motivations, definitions and simple examples will be introduced by the instructor.

1 Lesson 1 - October 25, 2014

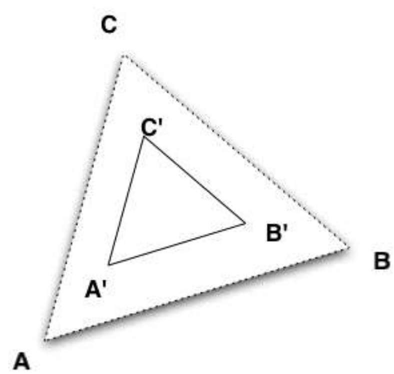
1.1 Symmetries of an equilateral triangle

Definition 1.1. An **equilateral triangle** is a triangle whose three sides are all of equal length. The below triangle ABC is an example of an equilateral triangle.

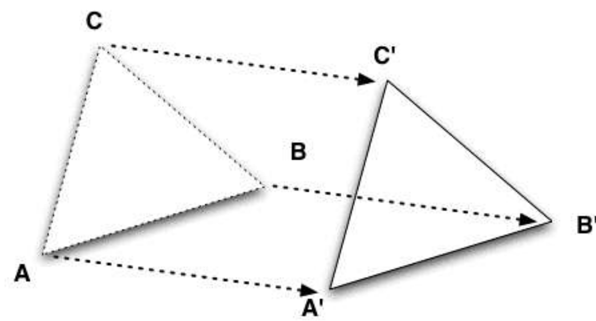


Main object: An equilateral triangle with corners labelled A, B, and C. Consider the following transformations:

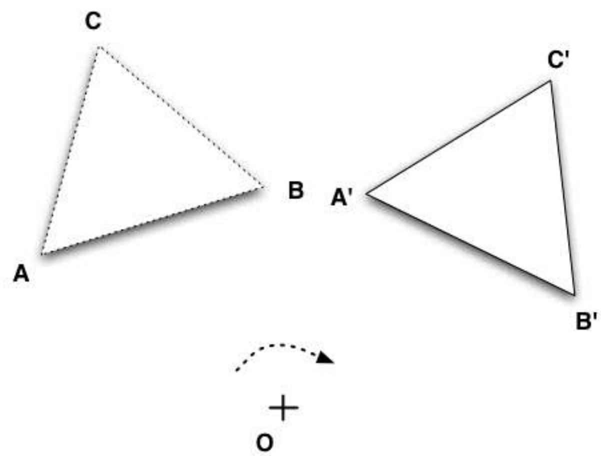
1. Scaling.



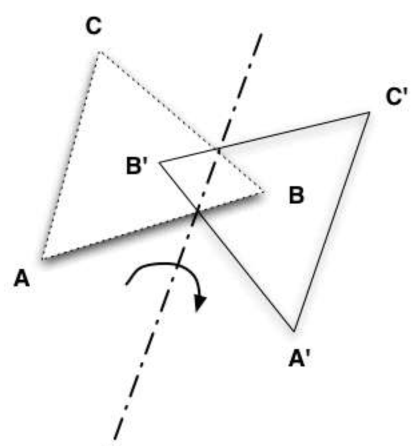
2. Translation.



3. Rotation.



4. Refection.

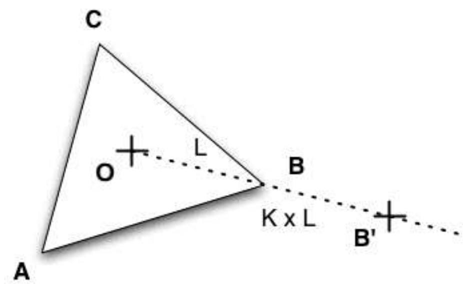


Which of these transformations leave our equilateral triangle invariant? Invariant here means that the *image of the new triangle after the transformation and the image of the original triangle* **overlap**.

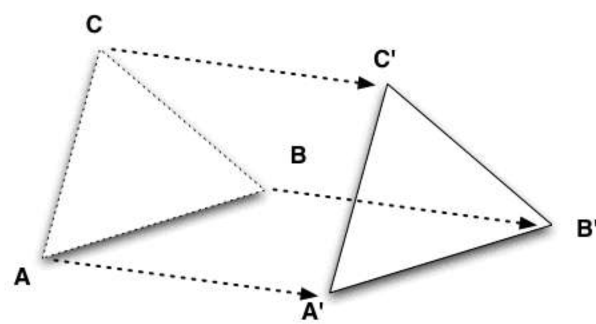
Definition 1.2. We call the transformations that leave the equilateral triangle invariant the **symmetries** of that triangle.

Let's examine all the symmetries of the triangle.

1. Scaling.

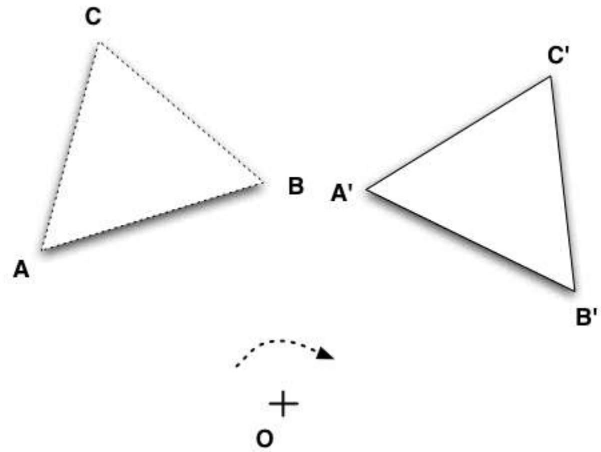


2. Translation.



Question 1.3. Suppose we compose two transformations, $T1$ first then $T2$, and suppose also that we get the trivial transformation. An example of this situation would the two translations mentioned earlier: translate "to the left" and then "back to the right". A natural question that arises is whether we still get the trivial transformation if we compose the transformations in reverse order? In this translation example, the answer is clearly yes. Is always the case when we compose two transformations?

3. Rotation.



Question 1.4. Make those two symmetries explicit by finding the rotation angles. Let us call these symmetries $R2$ and $R3$, where $R2$ is obtained by rotating by a smaller counter-clockwise angle.

Question 1.5. *Consider the following questions:*

(i) What is special about $R3$? Reprhase this using the trivial transformation language. Let us look at the first symmetry R1 we have found: we rotate the triangle around its center by 120° counter-clockwise. What happens when we compose $R1$ and $R1$, that is to say we do $R1$ twice in a row. Compare the composition symmetry with $R2$.

(ii) What happens now if we compose $R1$ three times in a row? Compare with $R3$.

(iii) What is the composition $R1$ then $R2$? How about $R2$ then $R1$? are they the same?

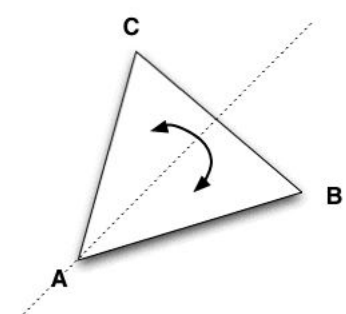
(iv) Rephrase the previous answer in terms of transformations that cancel each-other out and show how this gives another example of pairs of transformations that cancel each-other out no matter what order we compose them in.

Question 1.6. Suppose now we rotate the triangle 120° clockwise

(i) Show that this is also a symmetry of the triangle. Call it $R4$.

(ii) If we compose $R4$ with $R1$, we get the trivial transformation because that ends up rotating the triangle 120° counter-clockwise back to its original orientation. But we already know that composing $R1$ and $R2$ also give the trivial transformation. What kind of relationship is there between $R2$ and $R4$?

4. Refection.



Question 1.7. Show that in that case that the reflection axis goes through A and the middle of segment [BC] – you can use the fact that the triangle is equilateral and hence all 3 corners make 60* angles.

Summary: So far we have found the trivial transformation, 4 rotations and 3 reflections, and hence at least 8 symmetries. We said at least because we haven't studied the compositions of reflections and those of relections with rotations: those are all symmetris and could new ones we haven't listed yet. Here is the truth:
We have already seen when we studied rotations that $R3$ was trivial and $R4 = R2$ and hence we only have 2 rotations really, not counting the trivial one. Also, $R2$ was nothing but the composition of $R1$ with itself twice, and $R3$ the trivial rotation was also nothing but $R1$ composed three times with itlself.

$$R2 = R1 \circ R1, R3 = trivial = R1 \circ (R1 \circ R1).$$

where $X \circ Y$ means we compose X and Y by applying Y first then X second. Similarly, for reflection we have

$$XA \circ XA = XB \circ XB = XC \circ XC = trivial.$$

Question 1.8. What is $XA \circ XB$?

Question 1.9. What about $XC \circ XA$ and $XC \circ XB$?

Question 1.10. What is $XA \circ R2$? Then compare $XA \circ R2$ with $R2 \circ XA$.

Conclusion: We have observed the following:

(i) The symmetries form a set – we were able to list them all

(ii) Given two symmetries, we were able to compose them in a natural way – remember, they are just special transformations! – obtaining another symmetry.

(iii) There is a special symmetry, the trivial one, that is important because of the following point.

(iv) Given any of the symmetries, there is always another symmetry that cancels it out to the trivial symmetry by composition. For example $R1$ and $R2 = R1@R1$ cancel each other out. We do not know wether such a canceling symmetry is unique or not yet.

(v) We were able to find generators for the symmetries, although we did not phrase it that way. We showed (partially) that by doing various compositions of $R1$ and XA, we could cook out all of the other transformations. We say that $R1$ and XA are generators for the symmetries.

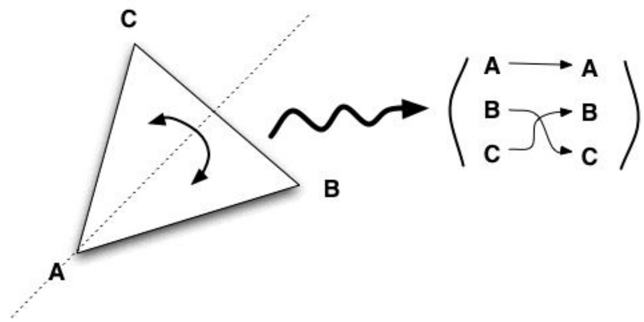
Question 1.11. List all possible symmetries of a square.

1.2 Permutations as a representation of symmetries

1.2.1 Permutations of 3 letters

Consider the reflection XA. It is simply a **permutation** of the vertices of the triangle: it shuffles them so that each vertex goes to one and only one new vertex, and no two vertices go the same new one. The standard mathematics notation for permutation is:

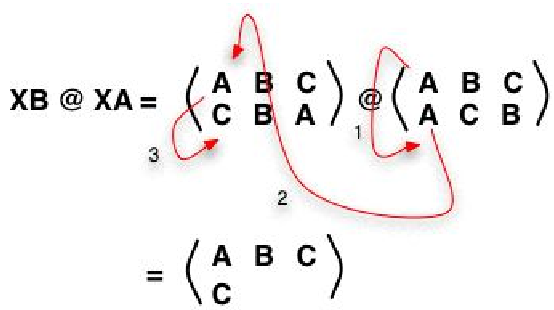
$$XA = \begin{bmatrix} A & B & C \\ A & C & B \end{bmatrix}.$$



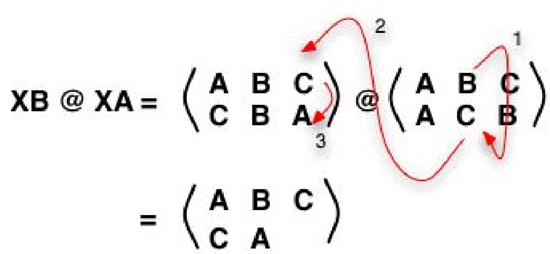
.

Question 1.12. What are the permutation notations for XB and $R1$?

So what happens to the composition of symmetries in this notation? We already know that $XB \circ XA = R2$. Well let's look at $X_B \circ X_A$. Remember we do X_A first then X_B. X_A takes A to A and then X_A takes that A to C. So we have the following sequence: (here @ is the same as $\circ$)



As to B, X_A takes it to C and then X_B takes that C to A again:



Question 1.13. Write down $XC \circ XA$ and check that $XC \circ XB = R2$ as well.

If we carry on the next step and following the path of C we get the desired permutation. Note that each symmetry gives a *different* permutation.

Question 1.14. But how many permutations of A, B and C are there all in all?

In summary we have 6 permutations in total, 6 of which come from symmetries of the triangle. In other words, every 3-permutation is the permutation associated to a symmetry of the triangle!

Question 1.15. Is the same true about the square?

1.2.2 Types of permutations

There are special types of permutations that we are going to study now.

Definition 1.16. A **transposition** is a permutation that only swaps two elements and leaves all the other ones unchanged

Question 1.17. What is an example of a transposition in our equilateral triangle example?

Definition 1.18. An **n-cycle** is a permutation that takes i_1 to i_2, i_2 to $i_3, \ldots$, i_{n-1} to i_n, i_n back to i_1 and leaves everything else unchanged. We write such permutation $(i_1 i_2 \ldots i_n)$.

Question 1.19. What is an example of a 3-cycle in our equilateral triangle example?

Remark 1.20. With the new notation of permutation, show composition permutation (123)(12) = (13). First, notice that for example (13)(24) = (24)(13). We say that those two cycles (they are transpositions in particular as you now know) are **disjoint**, meaning they permute two disjoint subsets of elements: the left-most ones swaps 1 and 3, while the second one swaps 2 and 4. The two subsets $\{1, 3\}$ and $\{2, 4\}$ are disjoint, they do not share any elements. Disjoint cycles always **commute**: the order in which we compose them does not matter, we always get the same answer.

We show now on an example how to re-write a composition of non disjoint permutations into a composition of disjoint cycles which is equal to it. Consider the composition (123)(124). These two cycles are not disjoint but the following algorithm will allow us to rewrite it as a disjoint composition:

1. Start with 1. The first permutation takes 1 to 2 and the second one takes that 2 to 3. We write (123)(124) = (13?
2. Next we look at 3. The first permutation takes 3 to 3, and then we take 3 to 1 and we have completed a cycle. We write (123)(124) = (13)?
3. After we complete a cycle, we start another cycle with the next free number. In this case, with start with 2. We write (123)(124) = (13)(2?
4. The first permutation takes 2 to 4, and then the second one takes that 4 to 4. We write (123)(124) = (13)(24?
5. Finally, the first permutation takes 4 to 1 and the second one takes 1 to 2 and we have completed a cycle. We write (123)(124) = (13)(24).
6. There are no remaining numbers and we are done!

1.2.3 Generators

We showed that XA and XB generated all those permutations. Now identifying A, B and C with $1, 2$ and 3 respectively, XA corresponds to (23) and XB to (13). Let us check that they do generate all those permutations:

- (123) is the composition (23)(13)
- (132) is the composition (13)(23)
- (12) is (13)(123) = (13)(23)(13)
- (13) is just (13)
- (23) is also just (23)

Question 1.21. Show that the rotations correspond in that identification to the permutations

$$(1234), (1234)(1234) = (13)(24), (1234)(1234)(1234) = (1432);$$

the diagonal reflections to (24) and (13); and the other reflections to (12)(34) and (14)(23).

Question 1.22. Write (1234) as a composition of (not necessarily disjoint) transpositions?

2 Lesson 2 - November 1, 2014

2.1 Quick overview of last lecture

2.2 Groups and its properties

We will begin to define what a group is and work on various examples.

Definition 2.1. A **group** is a set G with a binary operation $* : G \times G \to G$ such that:

1. The operation $*$ is associative. We say that an operation $*$ on a set X is *associative* if the following holds: for all x, y and z elements in X we have the following equality:

   $$x * (y * z) = (x * y) * z.$$

   In which case one simply writes $x * y * z$.

2. It has an identity element (and hence it has exactly one). An **identity** for an operation $*$ on a set X is an element e of X such that for all $x \in X$ we have

   $$x * e = e * x = x.$$

3. Every element in G has an inverse under $*$ (and hence a uniquely defined inverse). An inverse for x under $*$ is an element $y \in X$ such that:

   $$x * y = y * x = e.$$

Example 2.2. $(\mathbb{Z}, +)$ is an example of a group.

2.3 The set of all symmetries of an equilateral triangle is a group

Let S_T be the set of all symmetries of an equilateral triangle T. The composition of symmetries naturally gives S_T the structure of a set with a binary operation $\circ : S_T \times S_T \to S_T$. The binary operation satisfies the following special properties:

1. **Associativity:** To study this, we start with this question.

   Question 2.3. Compare $(R1 \circ R2) \circ X_A$ and $R1 \circ (R2 \circ X_A)$.

   Question 2.4. Which ones of the following operations are associative.

   (i) Addition on the real numbers. Multiplication on the positive real numbers.

   (ii) Division on the non-zero real numbers.

2. **Identity:** Another special property of ST is the existence of a particular element with a very special role: the trivial transformation. This transformation is such that when it is composed with any other transformation it leaves it identically unchanged.

Question 2.5. Suppose an operation $*$ on X has two identity elements e and f. Use the identity property for both e and f to simplify $e * f$ into two different expressions, and conclude that $e = f$ necessarily.

3. **Inverse:** Finally, recall that for every symmetry of the triangle, there was another symmetry that canceled it out. In other words, the symmetries are reversible transformations, one can always undo them. The following definition captures this idea. Let $*$ be an operation on X with identity e, and let x be an element in X.

Question 2.6. Let $X, *$ and e as in the previous definition but assume that $*$ is associative. Now let $x \in X$ with two inverses y and z. In other words, $x * y = y * x = e$ and $x * z = z * x = e$. Show that $z = z * (x * y) = (z * x) * y$ and conclude that $z = y$ and hence that an inverse under an associative operation is unique if it exists.

Question 2.7. Let $X, *$ and e as in the previous definition, but this time assume that X is finite, i.e. it only has finitely many elements, and that $*$ is associative. Now let $x \in X$ and $y \in X$ such that $x * y = e$. Consider the map $f : X \to X$ defined by $f(a) = y * a$ for $a \in X$.

(i) Show that f is **one-to-one**, a.k.a injective, by using an associativity trick on $x * f(a)$

(ii) Deduce that f is also onto because X is finite.

(iii) Deduce now that the previous statement implies that there exists an element $z \in X$ with $y * z = e$.

(iv) Show that $x = x * (y * z)$ implies that $x = z$ and $y * x = e$.

Question 2.8. Does the set of all symmetries of a square form a group?

Question 2.9. Does the set of all permutation of n elements form a group?

Question 2.10. Which one of these sets with operations are Groups?

1. The natural numbers with addition? With multiplication? How about substraction?
2. Same question with the rational numbers?

Forming a new group from old groups?

Question 2.11. Let $(\mathbb{Z}, +)$ be the additive integer group. Is $\mathbb{Z} \times \mathbb{Z} = \{(a, b) \mid a, b \in \mathbb{Z}\}$ a group? What would be its binary operation?

Question 2.12. Can you generalize this to any group $(G, *)$?

Question 2.13. Let M be the set of expressions of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c and d are real numbers. Define the binary operation $+$ on M by the following expression:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}.$$

Show that this operation makes M into a group. What is the identity in this case?

Question 2.14. Let O be the subset of M with elements $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $ad - bc \neq 0$, with operation $*$ defined:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} * \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}.$$

Show that this makes O into a group with identity. What is the identity in this case?

We will conclude the module with the rotational symmetries of a 3-dimensional cube. There are a total of 24 rotations of the cube.

Question 2.15. Can you find them all?

2.4 Appendix: Set Theory

Definition 2.16. A **set** is a collection of distinct objects.

Question 2.17. What are examples of sets that you have seen before?

There are two basic ways to represent a set.

1. The most basic way is to list all the elements in the set between curly braces. For example, the expression $\{2, 4, 6, 8, 10\}$ defines the set that contains the elements $2, 4, 6, 8$ and 10. If the given element does not appear in the list, it does to belong in the set.

2. The other way is to define sets as subsets of already defined sets. If X is an already defined set and P is a property that elemets in X may or may not have (we say of elements that have it that they satisfy P) , the expression $\{x \in X : x \text{ satisfies } P\}$ defines a set whose elements are all those elements of X that satisfy P. For example, assuming the set $\mathbb{N}$ of natural numbers was already defined, one can use the following notation $\{x \in N : x \text{ is divisible by } 17\}$ to denote all the natural numbers that are multiples of 17.

3. We write for the empty set.

There are also operations on sets. Given two sets S and T, one can define:

1. The **union**, denoted as $S \cup T$, of S and T: an element x belongs to $S \cup T$ if and only if it belongs to at least one of either S or T.

2. The **intersection**, denoted as $S \cap T$, of S and T: an element x belongs to $S \cap T$ if and only if it belongs to both S and T at the same time.

3. The **cartesian product**, denoted as $S \times T$: elements of are ordered pairs (s, t) where s is an element of S and t is an element of T.

For example, if $S = \{a, b\}$ and $T = \{b, c\}$, then $S \cup T = \{a, b, c\}$, $S \cap T = \{b\}$ and $S \times T = \{(a, b), (a, c), (b, b), (b, c)\}$.

2.4.1 Maps

Given two sets A and B, a **map** f from A to B is informally a way of associating elements in B to elements in A. A **well-defined map** (function) is a map from A to B satisfying the property that each element in A is associated with exactly one element in B. *From this point onward, we refer map as well-defined map.*

Given a set A, a binary operation $*$ is a map $* : A \times A \to A$. In other words, it is a device that takes pairs of elements in A as an input and outputs another element in A. One usually writes $a * b$ for $*((a, b))$, where a and b are elements in A.

Question 2.18. What are examples of binary operations that you have seen before?

For example, let A be the set $\{a, b, c\}$ then one can define a binary operation on A by filling the entries of a 3 by 3 table with elements in A.

Now suppose that we have two sets A and B, and two operations $* : A \times A \to A$ and $: B \times B \to B$. Suppose we also have a map $f : A \to B$. Given two elements in A, call them x and y, one can do the following actions.

1. First, we can combine x and y and look at $x * y$. This is another element in A and we can transform that into an element in B with f by calculating $f(x * y)$.

2. Second, one can transform x and y into elements in B by taking $f(x)$ and $f(y)$. One can them combine these two elements in B into yet another element in B by computing $f(x)^* f(y)$.

In general, there is no reason to expect that both recipes agree. In other words, there is no reason to have $f(x * y) = f(x) * f(y)$. Maps that satisfies this property are special and are called **homomorphisms** or simply **morphisms**. One also says of such a map that it agrees with the operations or that it is *compatible with them*. Given any random sets with operations, there might not be any homomorphism between them at all!

Question 2.19. Which ones of the following pairs form a pair of a set with a binary operation on it.

(i) The natural numbers with addition? With multiplication? With substraction? What about division? Rational numbers with multiplication? And division? What is special with 0?

(ii) The set of students in a classroom and the map that sends a pair of students to all the friends they have in common in that classroom? How to change the set and the map a little bit so that it becomes a binary operation? (Think of the set of subsets of students).

Question 2.20. More fun questions!

(i) Show that both the real numbers with addition, call them $(\mathbb{R}, +)$ and the real numbers with multiplication, $(\mathbb{R}, \times)$, form two pairs of a set with a binary operation. Do the same thing with the positive real numbers with multiplication.

(ii) Show that the map that sends a real number number to its double is a morphism of sets with operations from $(\mathbb{R}, +)$ to $(R, +)$. Can you find other examples? How about the map that sends a number to itself plus 5?

(iii) Show that the Exponential map is morphism of sets with operations for the right operations (The set is obviously that of the real numbers. Look at the operations you have, and see what happens when you apply the exponential).

(iv) Do the same thing with the Logarithm function.

References

[YS] http://www.math.cornell.edu/ mec/Summer2008/youssef/Groups/groups.html