Introduction to "Groups"

In mathematics we often consider a collection, or "set," of objects (such as our variations) that can be combined according to one or more rules. This rule, or list of rules, is called an "operation" defined on the set. A set, together with an operation defined on it, is called a "group" if it satisfies the following conditions:

- **Identity**: One of the objects in the set serves as the "identity" object of the set. This is an object that, when combined with any other object in the group, leaves that object unchanged.

- **Closure:** Whenever any two objects in the set are combined, the result is always an object in the same set. In other words, you can't "escape" from your set by combining objects in the set.

- **Opposites:** For any object in the set, there is some "opposite" object in the set that can be combined with the original set in order to end up with the set's "identity" object.

- **Associativity:** If any three objects in our set are being combined in a certain order, then the result is the same regardless of which of the other objects the middle (second) object of the three is combined with first.

Example: The set of 48 variations, under the rules for combining variations, is a "group."
The set has an identity (T_0), closure (the combination of two variations is always another variation in the set), and every variation has an opposite:

- T_n : For any n between 1 and 11, the opposite of T_n is T_{12-n}, since $T_n T_{12-n} = T_{12} = T_0$, and $n - 12$ will be between 1 and 11 when n is between 1 and 11.
  (On the other hand, the opposite of T_0 is just T_0 itself.)
- $T_n R$: The opposite of $T_n R$ is $T_{12-n} R$.
- $T_n I$: The opposite of $T_n I$ is $T_n I$.
- The opposite of $T_n IR$ is $T_n IR$.

Also, our set of rules is associative: for example, the result of combining $R\ T_n T_m$ will be the same regardless of whether we first combine R with T_n, or T_n with T_m.

> NOTE: In general, verifying the "associative" property is time-consuming and tedious, so we're not going to concern ourselves with it. Unless stated otherwise, all examples of a set with an operation defined on it will satisfy the "associativity" property.

Example: The set of numbers {0, 1, 2, … , n-1}, under "mod n" addition, is a "group."
We've seen a few examples of this in class and in homework assignments. Under "mod n" addition, we have a group in which 0 serves as the identity, and closure is guaranteed by the "mod n" rule itself, since by definition, every number is equivalent to some number in the range $0, 1, \dots, n-1$ under "mod n" arithmetic rules. As for opposites, the opposite of any number x (other than 0) would be $n - x$, since $x + (n - x) = n \equiv 0\ (mod\ n)$.

For example, under "mod 7" addition on the set {0, 1, 2, 3, 4, 5, 6}, the opposite of 1 would be 6, the opposite of 2 would be 5, and the opposite of 3 would be 4; 0 is its own opposite.

We will look at other examples of "groups" in class over the next few days.

One specific type of group, which occurs often and is of particular interest, is described below:

"Cyclic subgroup:" Any element of a group can be combined with itself repeatedly to generate a subgroup of the group in which it resides. (For our purposes, think of a "subgroup" as simply a smaller group contained inside of a larger group.) If a cyclic subgroup is generated by x, then we can write $< x >$ as a shorthand for the subgroup generated by x.

Examples of "cyclic subgroups" of the group of variations:

- The variation T_4 generates the cyclic subgroup $\{T_4, T_8, T_0\}$. That is, $T_4T_4 = T_8$, and then $T_8T_4 = T_0$. So, $< T_4 > = \{T_4, T_8, T_0\}$
- Combining T_3R with itself repeatedly gives us the results T_6, T_9R, and then T_0. So, $< T_3R > = \{T_3R, T_6, T_9R, T_0\}$.

The number of elements in the cyclic subgroup generated by a group element is called that element's "order" in the group. So, based on the above examples, T_4 would have order 3 (since its cyclic subgroup contains three distinct elements), and T_3R would have order 4.

Note that the cyclic subgroup is finished once repetition of our original group element results in the identity for that group. So, another way to describe the "order" of a group element is as the number of times that element can be repeated (that is, combined with itself) before the result is the identity element of the group.

Example: the inversion, I, has "order" 2, since $II = T_0$. That is, it just takes two inversions to arrive back at the identity variation, so the inversion's "order" is 2.

Another example: consider the group {0, 1, 2, … , 16, 17} under mod 18 addition. (As noted earlier, this is a "group.") The subgroup generated by 3 would be found as follows:

- Start with **3** itself
- Since our operation is mod 18 addition, add 3 to itself: 3+3=6, so we include **6** in our subgroup.
- Add 3 again: 6+3=**9**
- Add 3 again: 9+3=**12**
- Add 3 again: 12+3=**15**
- Add 3 again: $15 + 3 = 18 \equiv \mathbf{0}\ (mod\ 18)$

At this point, we can stop, since adding 3 again would give us the same results we had before – 3, then 6, then 9, etc. The results repeat – this is the "cyclic" part of a "cyclic subgroup" – so we know there's no reason to continue the process. Thus, the "cyclic subgroup generated by 3" in this example would be $\{3, 6, 9, 12, 15, 0\}$. Using our notation for cyclic subgroups, we could write $< 3 > = \{3, 6, 9, 12, 15, 0\}$.

(Note: if you were to check – say, with a mod 18 addition table – you would find that this set does satisfy all of the requirements for a group under mod 18 addition.)

We've also shown that the element 3 has "order" 6 in the group {0, 1, 2, … , 16, 17} under mod 18 addition, since its cyclic subgroup consists of six distinct elements.