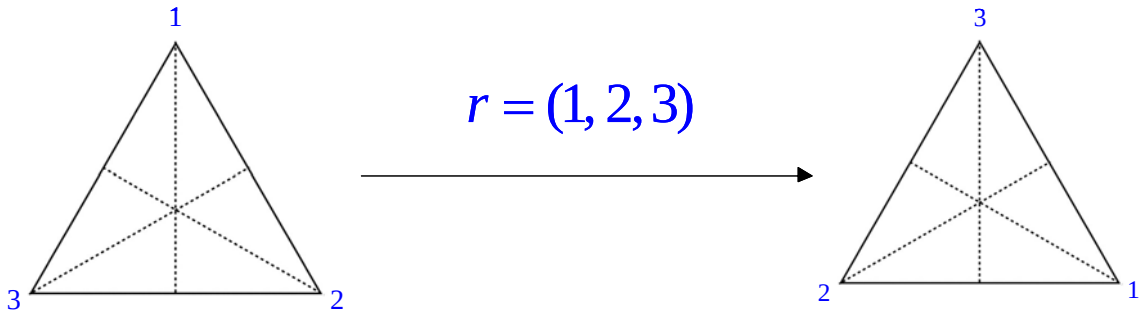
Lesson 2

CYCLIC GROUPS AND SUBGROUPS

In this section we are going to take a closer look at groups and cycles, and we'll encounter some new notation and definitions along the way. First, we'll revisit our equilateral triangle and we'll consider once again all the permutations and cycles that can be derived by rotating our triangle about its center through angles that are integer multiples of $120°$. Recall, also, that one clockwise rotation through $120°$ can be represented by the cycle $r = (1,2,3)$.



If we take this cycle, or any cycle for that matter, and keep repeating it (forwards and backwards), then we will always generate a group. And, in particular, the group we generate will be abelian. Recall that that means that all the elements of the group will commute with one another, i.e. we always have that $ab = ba$ for any elements *a* and *b* in our group. Recall, too, that if we keep repeating this cycle *r*, then we get the following, distinct results.

$r = (1,2,3)$

$r^2 = r^{-1} = (1,3,2)$

$r^3 = rr^2 = rr^{-1} = e = ()$

Thus, we can say that the group *G* generated consists of three elements, $e, r,$ and r^2, or in terms of permutations, $(), (1,2,3),$ and $(1,3,2)$. In particular, we can say that the group is generated by taking integer powers, positive and negative with $r^0 = e = ()$, of *r*, and to indicate the group generated by *r*, we write $\langle r \rangle = G = \{e, r, r^2\} = \{(), (1,2,3), (1,3,2)\}$. The number of elements in a group is called its size or order, and for the most part, we will primarily be examining just groups of finite order, since they are more likely to apply to what we encounter in the real world. The notation we use for the order of a group is a pair of absolute value signs. Thus, in this example we can say that $|G| = |\langle r \rangle| = 3$. Notice that if we look at the group generated by $r^2 = (1,3,2)$, we get back the same thing.

$r^2 = (1,3,2)$

$(r^2)^2 = (1,3,2)(1,3,2) = (1,2,3)$

$(r^2)^3 = r^2(r^2)^2 = (1,3,2)(1,2,3) = (1)(2)(3) = e = ()$

Thus, $\langle r \rangle = \langle r^2 \rangle$, and this means that different elements can generate the same group.

Now if we look at the group generated by *e*, we get a different story.

$e = (1)(2)(3) = ()$

$e^2 = (1)(2)(3) \cdot (1)(2)(3) = () \cdot () = ()$

… and so on

In other words, the group generated by *e* contains only one element, $\langle e \rangle = \{e\} = \{()\}$. This may seem rather trivial, and that is exactly why we call this the trivial group. Furthermore, since $\langle e \rangle = \{()\} \subseteq G = \{(), (1,2,3), (1,3,2)\}$ is a group contained within the larger group *G*, we call $\langle e \rangle$ a subgroup of *G*, and we write $\langle e \rangle \leq G$. Notice that every group always has two subgroups, itself and the identity. Furthermore, taking any element (or elements) in a group *G* and looking at all possible integer powers of that element (both positive and negative and zero, and where a negative power always indicates an inverse) will always generate a subgroup of *G*.

Now here are a few more details. Any group generated by a single element is called a cyclic group, and a cyclic group is always, always abelian. Thus, $\langle r \rangle = \{e, r, r^2\} = \{(), (1,2,3), (1,3,2)\}$ is a group of order 3 that is both cyclic and abelian. Furthermore, we can, for convenience, create a multiplication table for this group.

*	()	(1,2,3)	(1,3,2)
()	()	(1,2,3)	(1,3,2)
(1,2,3)	(1,2,3)	(1,3,2)	()
(1,3,2)	(1,3,2)	()	(1,2,3)

In terms of $e, r,$ and r^2, we can also write this as follows.

*	e	r	r^2
e	e	r	r^2
r	r	r^2	e
r^2	r^2	e	r

If we look at this latter multiplication table and highlight the diagonal from upper left to lower right, then we notice that the triangle below this diagonal is the mirror image of what's above. This always happens when the group is abelian, and, thus, if we have a multiplication table in front of us for a group, then we can always tell from the table whether or not our group is abelian.

*	e	r	r^2
e	e	r	r^2
r	r	r^2	e
r^2	r^2	e	r

When our group is cyclic, generated by just a single element, we often denote that group by C_n, C for cyclic and n for the number of elements in the group. Also, since our focus is mainly on finite groups, we'll assume that n is a finite number.

Below now are a few cyclic groups along with their multiplication tables.

$C_1 = \langle () \rangle$

*	()
()	()

$C_2 = \langle (1,2) \rangle$

*	()	(1,2)
()	()	(1,2)
(1,2)	(1,2)	()

$C_3 = \langle (1,2,3) \rangle$

*	()	(1,2,3)	(1,3,2)
()	()	(1,2,3)	(1,3,2)
(1,2,3)	(1,2,3)	(1,3,2)	()
(1,3,2)	(1,3,2)	()	(1,2,3)

$C_4 = \langle (1,2,3,4) \rangle$

*	()	(1,2,3,4)	(1,3)(2,4)	(1,4,3,2)
()	()	(1,2,3,4)	(1,3)(2,4)	(1,4,3,2)
(1,2,3,4)	(1,2,3,4)	(1,3)(2,4)	(1,4,3,2)	()
(1,3)(2,4)	(1,3)(2,4)	(1,4,3,2)	()	(1,2,3,4)
(1,4,3,2)	(1,4,3,2)	()	(1,2,3,4)	(1,3)(2,4)

Now let's take the last group, C_4, and let's look to see what cyclic subgroups are generated by the elements in C_4. Here's what we get.

$\langle () \rangle = \{ () \}$

$\langle (1,2,3,4) \rangle = \{ (), (1,2,3,4), (1,3)(2,4), (1,4,3,2) \}$

$\langle (1,3)(2,4) \rangle = \{ (), (1,3)(2,4) \}$

$\langle (1,4,3,2) \rangle = \{ (), (1,4,3,2), (1,3)(2,4), (1,2,3,4) \}$

What we see in the above list is that the identity element just generates the identity element as a subgroup, $(1,2,3,4)$ and $(1,4,3,2)$ generate the whole group, but $(1,3)(2,4)$ generates a subgroup of order 2. Furthermore, notice that the order of each subgroup is a divisor of the order of the entire group. This is no accident! This is something that always happens and eventually we will prove it. For now, however, we will just take the following theorem as a given fact.

Lagrange's Theorem: If G is a finite group such that $|G| = n$ and if H is a subgroup of G such that $|H| = m$, then m divides n.

Thus, for example, if $|G| = 7$, then every nonidentity element must generate the entire group since the only divisors of 7 are itself and 1. Similarly, a group of order 10 can never have a subgroup of order 3 since 3 does not divide evenly into 10. Now we can also ask if the converse is true. In other words, if a number divides the order of a group, then does the group have to have a subgroup of that order? Unfortunately, the answer is no. However, there is a very powerful theorem that we'll prove much, much later that tells us that if a prime number raised to a power divides the order of a group, then the group must have at least one subgroup with that prime power order.

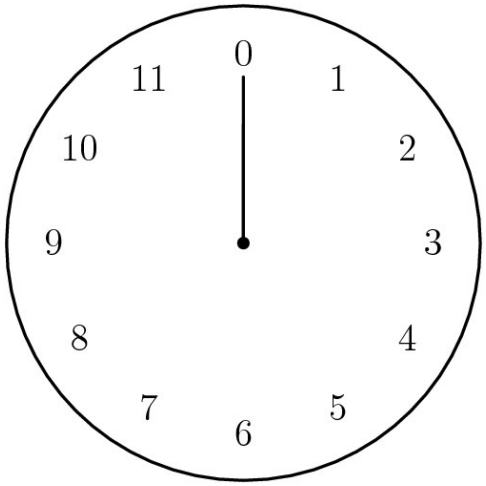
Theorem: If G is a finite group such that $|G| = n$ and if p is a prime such that p^m divides n for some natural number m, then G has a subgroup of order p^m.

For example, if $|G| = 24$, then we don't necessarily know that G has a subgroup of order 6, but we do know that G has subgroups of order $1, 2, 2^2, 2^3, 3$ and 24, and that in itself is very powerful knowledge about the internal structure of our group. And we also know that G does not have any subgroups of order 5 or 7 or any other number that doesn't divide evenly into 24. That's a lot of good stuff to know!

Another thing we should emphasize at this point is that in most of the examples above we have a set of numbers such as $X = \{1,2,3,4\}$ and then we have a group such as $G = C_4 = \{ (), (1,2,3,4), (1,3)(2,4), (1,4,3,2) \}$ that creates permutations of those numbers. It turns out that it is possible to represent all groups this way, as a collection of permutations of some set of objects X. In this type of representation, we say that the

group *G* acts on the set *X*, and this is a very practical way of thinking about groups that we want to become very familiar with.

And finally, I want to show you yet another way to think about cyclic groups that is also very common. Hopefully, many of you reading this have already been introduced to "clock arithmetic" which is nothing more than the kind of arithmetic we do with numbers on a clock. For example, if a clock says that it is 2 o'clock and if we add 3 hours to that time, then we arrive at 5 o'clock. However, if it is 10 o'clock and we add 3 hours to that time, then we just arrive back at 1 o'clock. On a clock, we can get up to 12 o'clock and then we start over again. However, when we do this kind of arithmetic in mathematics, it's much more convenient to replace 12 by 0.



Thus, using clock arithmetic with this clock, we can say that $2+3=5$, $10+3=1$, $6+6=0$, and $11+4=3$. We call this type of arithmetic "addition modulo 12," and an easy way to find the result is to just do ordinary addition and then check to see what the remainder is after dividing by 12. For example, under ordinary addition we have $11+4=15$ and 15 divided by 12 gives us a remainder of 3. Thus under addition modulo 12 (clock arithmetic) we have that $11+4=3$. Furthermore, if we take the set of numbers on our clock above, with 12 replced by 0, and add them together modulo 12, then we get a group that we call the integers modulo 12 that we denote by $\mathbb{Z}_{12}$.

Now for the good part! The integers modulo 12, $\mathbb{Z}_{12}$, is basically the same thing as the cyclic group C_{12}, and we can generate this group by taking the number 1 and adding on more ones until we get back to 0. Thus, when we talk about a cyclic group of order *n*, we can either think of that in terms of a particular set of permutations that correspond to *n* rotations about the center of a regular *n*-sided polygon, C_n, or we can think of it in terms of the integers modulo *n*, $\mathbb{Z}_n$. It's your choice!

And finally, below is a multiplication table for C_3 that we presented above, and next to it is a multiplication table for $\mathbb{Z}_3$. Notice that if we equate 0 with *e*, 1 with *r*, and 2 with r^2, then these tables are essentially the same. They basically represent the same cyclic group

of order 3. Only the labels for the elements have changed! And when we have two groups that are the same except for the labels used for the elements, then we say that the two groups are *isomorphic*. The word *isomorphic* essentially means *equal shape*.

*	e	r	r^2
e	e	r	r^2
r	r	r^2	e
r^2	r^2	e	r

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1