Lecture 11: Subgroups

Contents

Last lecture we introduced the concept of a *group*. This is a set equipped with an (associative) operation that allows us to combine two elements to produce another element in the same set. We require the set, under this operation, to have an identity, and for every element to have an inverse. We saw a number of familiar sets and operations which satisfy the property of being a group. In this lecture we look at subsets of groups.

11.1 Subgroups

Not all subsets of groups are created equal. For example, consider the two subset of the set of all Rubik's cube moves: $H = \{\varepsilon, \mathrm{R}, \mathrm{R}^2, \mathrm{R}^3\}$ and $K = \{\varepsilon, \mathrm{R}, \mathrm{U}\}$. The set H is a group itself as we saw last lecture. On the other hand, the set K is not a group since, for one thing the product of R and U is not in K.

If G is a group, and H is a subset of G which is also a group (using the same operation), then we say H is a **subgroup** of G, and we write $H < G$.

Example 11.1 *(a)* $H = \{\varepsilon, (1,2)\}$ *is a subgroup of* S_3.

(b) The subset $G = \{\varepsilon, (1,2,3,4), (1,4,3,2), (1,3)(2,4), (1,4)(2,3), (1,2)(3,4), (2,4), (1,3)\}$ *of* S_4 *is a subgroup. We could check that every product of elements in* G *is again in* G*, and that each element has an inverse in* G*. However, we could just observe that* G *is precisely* D_4*, the dihedral group of order 8 that we investigated last lecture, so we already know it is a group.*

(c) The subset $\{0,2,4\}$ *is a subgroup of the cyclic group of order* 6, $C_6 = \{0,1,2,3,4,5\}$.

To verify whether a subset of a group is itself a group we don't need to start from scratch. For instance, since the operation on G is associative, then restricting the operation to just elements of a subset H it would still have to be associative. This means we don't need to check associativity, we get this for free. So we really only need to check (i) H is closed, (ii) the identity is in H, and (iii) each element of H has an inverse in H. Notice that if we have (i) and (iii) then we get (ii) for free, since $aa^{-1} = e$. This means we have the following test for a subgroup.

Theorem 11.1 (Two-Step Subgroup Test) *Let G be a group and H a nonempty subset of G. If*

(a) for every $a, b \in H$, $ab \in H$ (closed under multiplication), and

(b) for every $a \in H$, $a^{-1} \in H$ (closed under inverses),

then H is a subgroup of G.

11.2 Examples of Subgroups

Imagine playing with Rubik's cube but only allowing yourself to use moves U and R. Some examples of move sequences that you could perform are: RU R^{-1} U^2 R^2 U^{-1}, RURURURUR, and $(\mathrm{R}^2\mathrm{U}^2)^3$. Observe that every move sequence has an inverse involving only R and U, and the product of any two move sequences is another move sequence involving only R and U. That is, the set of all such move sequences is a group! We denote this group by $\langle \mathrm{R}, \mathrm{U}\rangle$.

For any group G, let $g_1, g_2, \ldots, g_k$ be elements in G. Let $\langle g_1, g_2, \ldots, g_k\rangle$ be the set of all elements of G which can be expressed as products of $g_1, g_2, \ldots, g_k$ and their inverses $g_1^{-1}, g_2^{-1}, \ldots, g_k^{-1}$:

$$\langle g_1, g_2, \ldots, g_k\rangle = \{x \in G \mid x = g_{j_i}^{m_i} g_{j_2}^{m_2} \cdots g_{j_\ell}^{m_\ell} \text{ for some indices } j_i\text{'s and exponents } m_i \in \mathbb{Z}\},$$

then $\langle g_1, g_2, \ldots, g_k\rangle$ is the **subgroup generated by** $g_1, g_2, \ldots, g_k$.

When $k = 1$, the group $\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}$ is called a **cyclic** subgroup of G.

Many of our examples of subgroups will be of these types, and this is how we will construct groups in SAGE.

(1) Recall $S_3 = \{\varepsilon, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$.
One subgroup of S_3 is $\langle(1,2,3)\rangle = \{\varepsilon, (1,2,3), (1,3,2)\}$. Check this is indeed a subgroup.

We can list all subgroups of S_3 as follows:
$\langle\varepsilon\rangle = \{\varepsilon\}$
$\langle(1,2)\rangle = \{\varepsilon, (1,2)\}$
$\langle(1,3)\rangle = \{\varepsilon, (1,3)\}$
$\langle(2,3)\rangle = \{\varepsilon, (2,3)\}$
$\langle(1,2,3)\rangle = \{\varepsilon, (1,2,3), (1,3,2)\} = \langle(1,3,2)\rangle$

We can check that $\langle(1,2), (1,3)\rangle = S_3$. What this means is that any element of S_3 can be written as a product involving $(1,2)$ and $(1,3)$. In fact, the subgroup generated by *any two* elements will be all of S_3 again.

SAGE

```
sage: S3=SymmetricGroup(3)
sage: a=S3("(1,2)")
sage: b=S3("(1,3)")
sage: H=PermutationGroup([a,b])    # forms the group generated by a and b
sage: H==S3   # check if H is equal to the whole group
true
```

(2) Recall $C_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ and the operation is additional modulo 10. The subgroups of C_{10} are:
$\langle 0\rangle = \{0\}$
$\langle 2\rangle = \{0, 2, 4, 6, 8\}$
$\langle 5\rangle = \{0, 5\}$.
There are no other (proper) subgroups of C_{10}.

(3) Recall $U(10) = \{1, 3, 7, 9\}$ and the operation is multiplication modulo 10. Since $3^2 = 9$ and $3^3 = 7$ then $U(10) = \langle 3 \rangle$. A proper subgroup of $U(10)$ is $\langle 9 \rangle = \{1, 9\}$. Verify this is the only other proper subgroup of $U(10)$, besides the trivial subgroup $\{1\}$.

(4) In S_{10}, the permutations $\alpha = (1, 2)$ and $\beta = (1, 5, 3)(2, 4)$ generate a subgroup H of size 120. The permutation $(1, 4, 3, 2)$ is in H since $\alpha\beta\alpha\beta^2 = (1, 4, 3, 2)$. On the other hand, $(8, 9, 10) \notin H$, since any product of α and β would have to fix 10.

SAGE

```
sage: S10=SymmetricGroup(10)
sage: a=S10("(1,2)")
sage: b=S10("(1,5,3)(2,4)")
sage: H=PermutationGroup([a,b])    # could have used H=S10.subgroup([a,b]) instead
sage: H.order()
120
sage: a*b*a*b^2
(1,4,3,2)
sage: S10("(1,4,3,2)") in H
true
sage: S10("(8,9,10)") in H
false
```

(5) Some subgroups of the dihedral group $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$ are
$\langle R_{90} \rangle = \{R_0, R_{90}, R_{180}, R_{270}\}$
$\langle R_{180} \rangle = \{R_0, R_{180}\}$
$\langle V \rangle = \{R_0, V\}$
$\langle H, V \rangle = \{R_0, R_{180}, H, V\}$
If we construct only the portion of the multiplication table that involves $\{R_0, R_{180}, H, V\}$ then we can immediately see that it is a subgroup since it is closed under the operation, and inverses.

SAGE

```
sage: D4=DihedralGroup(4)
sage: D4sublist=["()","(1,3)(2,4)", "(1,4)(2,3)", "(1,2)(3,4)"]
sage: D4subnames=["R0","R180","H","V"]
sage: D4.cayley_table(names=D4names,elements=D4list)
 *    R0 R180    H    V
    +--------------------
  R0|   R0 R180    H    V
R180| R180   R0    V    H
   H|    H    V   R0 R180
   V|    V    H R180   R0
```

11.3 The Center of a Group

The **center** of a group G is the subset $Z(G)$ of all elements that commute with every element of G:

$$Z(G) = \{a \in G \mid ag = ga \text{ for all } g \in G\}.$$

Theorem 11.2 *For a group G the center $Z(G)$ is a subgroup of G.*

Proof: The identity is in $Z(G)$. If a and b are in $Z(G)$ then for any $g \in G$, $(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab)$ so $ab \in G$. Also, $ag = ga$ implies $ga^{-1} = a^{-1}g$ so $a^{-1} \in G$. Therefore, by the Two-Step subgroup test $Z(G) < G$.

$\square$

Note that $Z(G) = G$ if and only if G is abelian. We've shown in a previous exercise that for every non-trivial permutation in $S - n$, where $n \geq 3$, there exists one that does not commute with it. This means $Z(S_n) = \{\varepsilon\}$.

However, for subgroups of of S_n this is not necessarily the case. For example A_3 is abelian and so $Z(A_3) = A_3$. Here we verify this in SAGE.

SAGE

```
sage: A3=AlternatingGroup(3)
sage: A3.center()
Permutation Group with generators [(1,2,3)]
sage: A3.center().list()
[(), (1,2,3), (1,3,2)]
```

We'll use the center subgroup later on when investigating Rubik's cube.

11.4 Lagrange's Theorem

Looking back at our examples in last section we make the following observation: *the order of a subgroup divides the order of the group*. For example, in S_3, which is a group of order 6, all the subgroups we listed has either order 1, 2 or 3, which are precisely the divisors of 6. Verify this observation for the other examples.

The raises the question: Is this always the case? Must the order of a subgroup always be a divisor of the order of the group? If this is true, then it puts a pretty strict condition on the possible subsets that can be subgroups. For instance, we would be able to conclude pretty quickly that $\{R_0, H, D\}$ is not a subgroup of D_4 since 3 does not divide 8.

It turns out that our observation is true in general. This is known as Lagrange's Theorem.

Theorem 11.3 (Lagrange's Theorem) *If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.*

We will not prove this theorem here.

If we consider the subgroup $\langle g \rangle$ generated by an element $g \in G$, then the order of this subgroup is precisely the order of g. In other words, our two definitions of the word "order" (both as the size of a group, and the smallest number n for which $g^n = e$) agree.

Corollary 11.1 ($ord(a)$ divides $|G|$) *In a finite group, the order of each element divides the order of the group.*

Here is some experimental evidence in support of the corollary.

SAGE

```
sage: n=20
sage: Cn = CyclicPermutationGroup(n)
sage: element_orders=Set([g.order() for g in Cn])
sage: element_orders
{1, 2, 4, 5, 10, 20}
```

The orders of the elements in C_{20} are all divisors of 20. We could vary n, try dihedral groups or unit integer groups, etc. In every case, we would find that the order of an element must divide the order of the group.

As a partial converse to Corollary 11.1 we have the following.

Theorem 11.4 (Cauchy's Theorem) *Let p be a prime dividing $|G|$. Then there is a $g \in G$ of order p.*

Note that for non-prime divisors d of $|G|$ it is not true in general that G contains an element of order d. For example, $H = \{\varepsilon, (1,2), (3,4), (5,6), (1,2)(3,4), (1,2)(5,6), (3,4)(5,6)\}$ is a subgroup of S_6 of order 8, but it does not contain an element of order 4 or 8.

A proof of Cauchy's Theorem will be deferred to a later lecture (if we have time).

11.5 Cyclic Groups Revisited

In a cyclic group $G = \langle g \rangle$ every element is of the form g^k for some k. If G is infinite then every distinct power of g is a distinct element of G. Think about $\mathbb{Z} = \langle 1 \rangle$ under addition as an example (of course, here we have to reinterpret "power" to mean "multiple" since the group operation is addition),

If $G = \langle g \rangle$ is finite of order n then $G = \{e, g, g^2, \dots, g^{n-1}\}$ and $g^i = g^j$ if and only if $n \mid j - i$.

This means it is fairly easy to work with cyclic groups, since taking products and determining when two elements are really the same, is a fairly simple task.

The following theorems list some nice properties that cyclic groups have, including how to find all subgroups and all elements of a particular order.

Theorem 11.5 (Fundamental Theorem of Cyclic Groups) *Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle g \rangle| = n$ then for each divisor of k of n there is exactly one subgroup of $\langle g \rangle$ of order k.*

The proof of this is well within our reach, but I will not prove it here.

Theorem 11.6 (Generators of Cycle Groups) *Let $G = \langle g \rangle$ be a cyclic group of order n. Then $G = \langle g^k \rangle$ if and only if $\gcd(k, n) = 1$.*

Theorem 11.7 (Number of elements of each order in a cyclic group.) *If d is a divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.*

In the specific case when the group is C_n, and the operation is addition, these theorems can be restated as follows.

Theorem 11.8 (Generators, Subgroups, and Orders in C_n) *Consider the group of integers modulo n, C_n.*

(a) An integer k is a generator of C_n if and only if $\gcd(k, n) = 1$.

(b) For each divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of C_n of order k, moreover, these are the only subgroups of C_n.

(c) For each $k \mid n$ the elements of order k are $\ell \cdot (n/k)$ where $\gcd(\ell, k) = 1$. The number of such element is $\phi(k)$, and each of these is a generator of the unique subgroup of order k.

Example 11.2 *Let's determine all the subgroups of C_{24}. By Theorem 11.8 the generators of C_{24} are precisely the elements which are relatively prime to $24 = 2^3 3$. These are $1, 5, 7, 11, 13, 17, 19, 23$.*

$\langle 1 \rangle = C_{24}$

2 is an element of order 12, so it generates a cyclic subgroup of order 12:

$\langle 2 \rangle = \{0, 2, 3, 6, 8, 10, 12, 14, 16, 18, 20, 22\}$.

The other generators are $k \cdot 2$ where k is relatively prime to 12. Since there are $\phi(12) = 4$ numbers relatively prime to 12, namely $\{1, 5, 7, 11\}$ then the other generators of this subgroup are $5 \cdot 2 = 10$, $7 \cdot 2 = 14$, $11 \cdot 2 = 22$.

3 is an element of order 8, so it generates a cycle subgroup of order 8:

$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21\}$.

Other generators of this subgroup are $m \cdot 3$ where m is relatively prime to 8. There are $\phi(8) = 4$ such generators: $3, 9, 15, 21$.

subgroup	order	other generators
$\langle 1\rangle = C_{24}$	24	$5, 7, 11, 13, 17, 19, 23$
$\langle 2\rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22\}$	12	$10, 14, 22$
$\langle 3\rangle = \{0, 3, 6, 9, 12, 15, 18, 21\}$	8	$9, 15, 21$
$\langle 4\rangle = \{0, 4, 8, 12, 16, 20\}$	6	20
$\langle 6\rangle = \{0, 6, 12, 18\}$	4	18
$\langle 8\rangle = \{0, 8, 16\}$	3	16
$\langle 12\rangle = \{0, 12\}$	2	
$\langle 0\rangle = \{0\}$	1	

Table 1: Subgroups of C_{24}

We can continue looking for subgroups (and generators) in this way. We just keep in mind that to find a subgroup of size k we look for an element of order k, since it will generate the only subgroup of size k. This is what Theorem 11.8 (and more generally Theorem 11.5) states.

Table 1 lists all subgroups, orders and generators of C_{24}.

11.6 Cayley's Theorem

We've mostly been focussing our attention on permutation groups. One may wonder whether we are limiting ourselves, and missing out on some pretty important groups that we wouldn't otherwise see. Well, it turns out that *every* group is really just a permutation group, the difference is only in the names. To see this, let G be a finite group of order n. List the elements of G:

$$g_1, \quad g_2, \quad g_3, \quad \cdots \quad , g_{n-1} \quad , g_n.$$

For any element $a \in G$ multiply the elements of the list by a:

$$ag_1 \quad , ag_2, \quad ag_3, \quad \ldots, \quad ag_{n-1}, \quad ag_n.$$

This is just a permutation of the list of elements in G. In other words, we can associate to the element a the permutation that it induces on the elements of G. It turns out that the set of all such permutations contains all the information about G. In other words, we can just think of G as a set of permutations. This is known as Cayley's theorem.

Theorem 11.9 (Cayley's Theorem) *Let G be a group. For each $a \in G$, define a mapping*

$$\begin{aligned} \rho_a :\ & G \to G \\ & x \mapsto ax. \end{aligned}$$

Then

(a) ρ_a is a permutation of the set G,

(b) $H = \{\rho_a \mid a \in G\}$ is a subgroup of S_G, the group of all permutations of the set G.

(c) H and G are essentially the same groups, all that is different is the names of the elements. More precisely, if $ab = c$ in G then $\rho_a\rho_b = \rho_c$ as permutations.

We only note the theorem here since it tells us that we aren't, in a sense, limiting ourselves by studying only permutation groups. Also, this theorem indicates why SAGE uses permutation groups to represent other groups.

11.7 Exercises

1. Is $\{\varepsilon, (1,2), (1,2,3)\}$ a subgroup of S_4?
2. We name the elements in S_3 as follows:

$$s_1 = (1,2), \quad s_2 = (1,3), \quad s_3 = (2,3), \quad s_4 = (1,2,3), \quad s_5 = (1,3,2).$$

   (a) Let G be the subgroup generated by s_1, $G = \langle s_1 \rangle$. Verify there are only two elements in G.
   (b) What is the order of s_4?
   (c) Let H be the permutation group with generator s_5, $G = \langle s_5 \rangle$. Verify that there are only three elements in H.
   (d) Show that $S_3 = \langle (1,2), (1,3,2) \rangle$.
3. Let $G = \langle (1,2), (3,4,5) \rangle$. Show that G is a subgroup of S_5 of order 6.
4. Find a subgroup of order 4 in S_4.
5. Find a subgroup of order 8 in S_4.

Dihedral Groups:

6. Determine all the subgroup of D_3.
7. Find the center $Z(D_4)$ of D_4.
8. Determine all the subgroup of D_5.
9. (a) Determine the number of elements of order 2 in D_n.
   (Hint: You will need to consider the cases n is even and n is odd separately.)
   (b) How many subgroups of order 2 does D_n have?
10. Determine the orders of the elements in D_{33} and how many there are of each.
11. How many elements of order 4 does D_{12} have? How many elements of order 4 does D_{4n} have.

Group of Integers under addition modulo n:

12. Find all the subgroups, and determine generators for each subgroup, for each of the following.

   (a) C_8 (b) C_{12} (c) C_{17}

13. Find all the elements of order 6 in C_{18}.
14. Find all the elements of order 15 in C_{30}.
15. Find all the elements of order 10 in C_{40}.

16. List all the elements of order 8 in $C_{8000000}$.

Unit Group modulo n:

17. Determine all the subgroups of $U(12)$.
18. For each value of n listed below, determine whether or not $U(n)$ is a cyclic group. When it is cyclic, list all of the generators of $U(n)$, $n = 5, 9, 10, 14, 15, 18, 20, 22, 25$. Make a conjecture about the prime power decomposition of integers n for which $U(n)$ is cyclic. Are $n = 9$ and $n = 16$ counterexamples of your conjecture? (Try them.) If so, modify your conjecture.
19. Given the fact that $U(49)$ has 42 elements, determine the number of generators that $U(49)$ has without actually finding any of the generators.
20. Prove that $U(2^n)$ ($n \geq 3$) is not cyclic.

    (Hint: Look for a property that $U(2^n)$ has that cyclic groups do not have.)

Subgroups in General:

21. Prove that a group of order 3 must be cyclic.
22. Suppose that G is a cyclic group and the 6 divides $|G|$. How many elements of order 6 does G have? If 8 divides $|G|$, how many elements of order 8 does G have? If a is one element of order 8, list the other elements of order 8.
23. Let $|G| = 33$. What are the possible orders for the elements of G? Show that G must have an element of order 3.
24. Let $|G| = 8$. Show that G must have an element of order 2. Show by counterexample that G need not have an element of order 4.
25. If G is an abelian group and contains cyclic subgroups of orders 4 and 5, what other sizes of cyclic subgroups must G contain.
26. If G is an abelian group and contains a pair of subgroups of order 2, show that G must contain a subgroup of order 4. Must this subgroup be cyclic?
27. Show that every group of order at most 4 is abelian. This says that groups of order ≤ 4 don't have enough room to have elements that don't commute.
28. Show that if G is a group where $|G| = p$ is prime then G is cyclic.
29. **One-Step Subgroup Test**. Let G be a group and H a nonempty subset of G. Show that H is a subgroup of G if $ab^{-1} \in H$ for every $a, b \in H$.
30. **Finte Subgroup Test** Let G be a finite group and H a nonempty subset of G. Show that H is a subgroup of G if H is closed under multiplication.