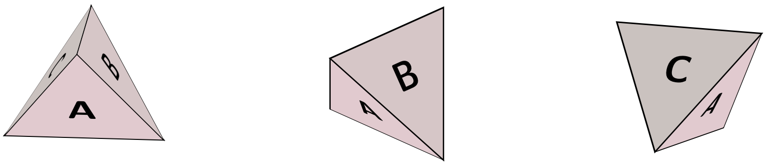
Fundamentals of Pure Mathematics
Week 3 workshop. How common are subgroups?

The point of this workshop is to gain some intuition for the statement 'let G be a group, with subgroup H'.

Let $(G, *)$ be a group. Recall that a non-empty subset H of G is called a *subgroup* if H is itself a group (under the operation $*$).

To determine what is true and false about subgroups, we require some examples:

Example 1. Recall that the regular tetrahedron is the Platonic solid

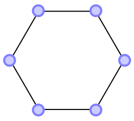


Let T denote the group of rotational symmetries of the tetrahedron.

(a) Determine $|T|$ (note: later in the course, once we learn the orbit–stabilizer theorem, this will be a bit easier).

(b) List explicitly all the elements of T.

Example 2. Recall that the regular 6-gon (=hexagon) is



Let D_6 denote the group of symmetries of the regular 6-gon.

(a) Determine $|D_6|$.

(b) List explicitly all the elements of D_6.

Example 3. Consider the group $A := \mathbb{Z}_{12}$.

(a) List explicitly all the elements of A.

(b) Determine $|A|$.

Now if G is an arbitrary finite group, we are interested in whether there are 'easy' ways of determining whether subgroups of G exist. Also, how often do they appear? In the statement 'let G be a group, with subgroup H', we are assuming that H exists — how strong is this assumption? Is our theory empty? The above three examples will help us gain some intuition into this problem.

Question 1. Let G be a finite group.

(a) There are always two subgroups of G. What are they?

(b) Prove that if $g \in G$, then $\langle g \rangle$ is a subgroup of G (thus every element of G generates a subgroup).

(c) Prove the following: if $|G| > 1$ is not prime, then G has a subgroup other than those in (a).

Hence, from (b), there is a procedure, given any element, to produce a subgroup. This however may result in one of the subgroups from (a). Part (c) says that provided the order of G is not prime[1], there exist other subgroups. Our theory is thus non-empty.

Question 2. Let's apply Question 1 to the Examples 1–3.

(a) In Example 1, for each element in T describe (i.e. list the elements in) the subgroup that it generates. How many different subgroups do you get, and how many elements does each subgroup have?

(b) Try the same question on Examples 2 and 3. Do you get the same answer in Examples 1–3?

(c) Next week we will learn Lagrange's Theorem, which states that the order of a subgroup must divide the order of the group. Quickly check that in your answers to (a) and (b), this property is satisfied.

You should now have quite a few examples of subgroups, and we know that the order of any such subgroup must divide the order of the group. Optimistically, we can ask whether the converse also holds.

Question 3. Let G be a finite group, and suppose that n divides $|G|$. Then does there exist a subgroup of order n?

(a) If you are optimistic that this is true, give a proof.

(b) If you are less optimistic (or don't have any feeling about it), it is best to check some examples first. In Examples 1–3, is the statement true? (Note at this stage the subgroups you have produced in Question 2 are all *cyclic* — there might be others!)

(c) By going between the approaches in (a) and (b), try to determine whether the statement is true or false.

Final remark: if we let $|G| = p_1^{a_1} \dots p_n^{a_n}$ be the prime decomposition of $|G|$ (where the p_i are distinct primes), it turns out that there is always a subgroup of order $p_i^{a_i}$. This is the content in The First Sylow Theorem, which we may cover later in the course (as an application of Group Actions).

[1] Note that if $|G|$ is prime, then G is cyclic, and so easy to understand. Hence $|G|$ not being prime is a rather mild assumption.

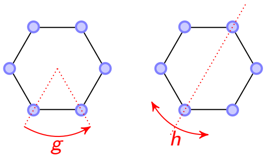
Ex1. (a) Pick face A. A rotational symmetry must take A to another face (i.e. an element of the set $\{A, B, C, D\}$), of which there are 4 choices (and each choice is possible). Once this has been established, the remainder of the symmetry is determined by where $\{B, C, D\}$ get sent. There are three options, corresponding to the three rotations around A. Hence overall there are $4 \times 3 = 12$ rotational symmetries.

Proof after we know orbit–stabilizer: Pick face A. Then the orbit of A contains all the other faces (the action is transitive), so $|\mathrm{Orb}_G(A)| = 4$. On the other hand the only way that A is fixed under a rotational symmetry is if the tetrahedron rotates around A, of which there are precisely three rotations, so $|\mathrm{Fix}(A)| = 3$. Hence by orbit–stabilizer $|G| = |\mathrm{Orb}_G(A)| \times |\mathrm{Fix}(A)| = 4 \times 3 = 12$.

(b) We first have the identity. We then have two non-trivial rotations fixing A, two non-trivial rotations fixing B, two non-trivial rotations fixing C and two non-trivial rotations fixing D. This gives 8 elements, each of order 3. With the identity, this adds up to 9 elements so far. The other three symmetries are 'half-rotations about the centres of opposite edges' (there are three sets of opposite edges), and each of these has order 2.

Ex2. (a) (This is very similar to Workshop 1). Label the vertices $1, \dots, 6$. Any symmetry must preserve vertices of valency two, so must take the vertex 1 to a member of the set $\{1, 2, \dots, 6\}$. Any such choice is possible, and after making this choice (there are six possible), everything else is determined by whether the neighbours of 1 are fixed or swapped (of which there are two choices). Hence there are $6 \times 2 = 12$ symmetries in total.

(b) If we denote



then as in lectures

$$D_6 = \{e, g, \dots, g^5, h, gh, \dots, g^5 h\}.$$

Ex3. $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ and $|\mathbb{Z}_{12}| = 12$.

Q1 (a) $\{e\}$ and G.

(b) In lectures, we defined $\langle g \rangle$ to be the set consisting of all possible powers (positive, negative and zero) of g. We use the test for a subgroup. Since $g \in \langle g \rangle$, the set $\langle g \rangle$ is not empty. Now take two arbitrary elements g^a and g^b in $\langle g \rangle$, then $g^a g^b = g^{a+b}$ also belongs to $\langle g \rangle$. Finally, for an arbitrary element $g^a \in \langle g \rangle$, the inverse is g^{-a}, and it also belongs to $\langle g \rangle$. Hence $\langle g \rangle$ is a subgroup.

(c) If G is not cyclic, pick $e \neq g \in G$. Since G is not cyclic, g cannot have order $|G|$, so $\langle g \rangle \neq G$. Since $e \neq g$, we also have $\{e\} \neq \langle g \rangle$.

If G is cyclic, say $G = \langle g \rangle$. Since $|G|$ is not prime, write $|G| = ab$ with $a, b > 1$. Consider g^a. This has order $b < |G|$, so $\langle g^a \rangle \neq G$. Since $g^a \neq 1$, we also have $\{e\} \neq \langle g^a \rangle$.

In either case, there is a subgroup different from $\{e\}$ and G.

Q2. (a) The identity generates the subgroup $\{e\}$. Each element of order 3 generates a cyclic subgroup of order 3, and each half-rotation generates a cyclic subgroup of order 2. The number depends on how you count — if you count up to isomorphism you get three 'different' subgroups (namely $\{e\}$, the cyclic group of order two, and the cyclic group of order three). If you count up to equality of sets, both non-trivial rotations that fix the same face generate the same set. Hence we get

$$\underbrace{1}_{\text{identity}} + \underbrace{4}_{\text{fix faces}} + \underbrace{3}_{\text{half-rotation}} = 8$$

different subgroups.

(b) For Example 2, let g and h be defined as in the answer to Ex2(b). The subgroup generated by e is always $\{e\}$. The subgroup generated by g is equal to the subgroup generated by g^5, which is equal to $\{e, g, \dots, g^5\}$, the cyclic group of order 6. The subgroup generated by g^2 is equal to the subgroup generated by g^4, which equals $\{e, g^2, g^4\}$, the cyclic group of order 3. The subgroup generated by g^3 is $\{e, g^3\}$, the cyclic group of order 2. Each of the reflections generate a cyclic group of order 2. As sets, we get thus get

$$\underbrace{1}_{\text{identity}} + \underbrace{3}_{\text{from rotations}} + \underbrace{6}_{\text{from reflections}} = 10$$

different subgroups. Up to isomorphism we get four (namely $\{e\}$, the cyclic group of order two, the cyclic group of order three and the cyclic group of order six).

For Example 3 we get $\mathbb{Z}_{12}$ (generated by 1 and more generally by any n with $\gcd(n, 12) = 1$), $\{0, 2, 4, 6, 8, 10\}$ (generated by any n with $\gcd(n, 12) = 2$), $\{0, 3, 6, 9\}$ (generated by any n with $\gcd(n, 12) = 3$), $\{0, 4, 8\} = \langle 4 \rangle = \langle 8 \rangle$, and $\{0, 6\} = \langle 6 \rangle$.

Q3. In Example 1, there is no subgroup of order 6. This can be done directly, but is not particularly pleasant.

Solution 1. Say that N is a subgroup of order 6. It must contain the identity. Suppose that it also contains all the elements of order 2. There are only three of these, hence so far we have only four elements. From our list of elements, there must be at least one rotation (of order 3) in N, and its square must also be in N (since N is closed under composition). You have to convince yourself (using the tetrahedron) that this set is not closed under composition, which gives a contradiction.

Hence the assumption that N contains all the elements of order 2 is false. Since the composition of any two of the half-rotations is the other half-rotation, this means that N can only contain at most one half-rotation (and also the identity). This means that it must contain at least four more elements, and so this forces inside N two rotations about different faces, and their squares. Again, you have to convince yourself (using the tetrahedron) that this set is not closed under composition, which gives a contradiction. This proves the result, in a rather painful way.

Solution 2. Here is a proof once we know about cosets (note that it has very little to do with the tetrahedron): let N be a subgroup of order 6, then since $\frac{|G|}{|N|} = 2$, N has only two distinct left cosets. Consider any element $g \in G$ of order three, and consider the left cosets

$$N, gN, g^2N.$$

Since there are only two distinct left cosets, two of these must be equal. If $N = gN$ then by rules for cosets $g \in N$. If $gN = g^2N$ then again by rules for cosets $g \in N$. Finally, if $N = g^2N$ then $g^2 \in N$, so since N is a subgroup $g^2g^2 \in N$, so $g^2g^2 = g^4 = g \in N$.

Hence in all cases $g \in N$. Since g is an arbitrary element of order 3, this shows that N contains all the elements of order 3. But we already know that there are eight of these, which contradicts the fact that $|N| = 6$. Hence N cannot exist.