MTH101: Symmetry
Tutorial 02

Problem 1. List all groups of order 6 and 7 up to isomorphism.

Solution.
Groups of order 6: Let G be a group of order 6. By Lagrange's theorem, the order of an element of G might be 1, 2, 3 or 6.
Case 1: Suppose G has an element x of order 6.

Then, the subgroup $\langle x \rangle$ has 6 elements and so $G = \langle x \rangle$. In this case, the multiplication table is as follows:

	1	x	x^2	x^3	x^4	x^5
1	1	x	x^2	x^3	x^4	x^5
x	x	x^2	x^3	x^4	x^5	1
x^2	x^2	x^3	x^4	x^5	1	x
x^3	x^3	x^4	x^5	1	x	x^2
x^4	x^4	x^5	1	x	x^2	x^3
x^5	x^5	1	x	x^2	x^3	x^4

This is just the group of rotational symmetries of a regular hexagon. This ends the discussion of Case 1.

Suppose G does not have any element of order 6. Then, every non-identity element must have order 2 or 3.

Case 2: Suppose G does not have any element of order 6, but has an element of order 3.

Let us denote the element of order 3 by x. Then, the group $\langle x \rangle = \{1, x, x^2\}$ has only 3 elements and so does not exhaust the whole group G. So, there exists an element y which is not in $\langle x \rangle$. Then, the elements y, yx and yx^2 are all distinct and do not lie in $\langle x \rangle$. (To see this, you may use the arguments that were used in the lectures, or just use the fact that these are the three elements of the coset $y\langle x \rangle$, which is distinct from $\langle x \rangle$.) Thus,

$$G = \{1, x, x^2, y, yx, yx^2\}.$$

Since we have agreed that G does not have an element of order 6, the order of y must be equal to 2 or 3.

Suppose $ord(y) = 3$. Then, $y^2 \neq 1$. However, y^2 is one of the six elements listed above. If $y^2 = yx^i$ for some i, then we get $y = x^i$. However, we have assumed that y is not in $\langle x \rangle$. So, y^2 must be equal to x or x^2. If $y^2 = x$, then $yx = y^3 = 1$, which contradicts the fact that the six elements listed above are distinct. Similarly, if $y^2 = x^2$, $yx^2 = y^3 = 1$, which also cannot be true. Thus, we see that $ord(y) \neq 3$.

Thus, we conclude that $ord(y) = 2$. Now, we try to compute the rest of the multiplication table.

The element xy does not lie in the subgroup $\langle x \rangle$. So, it is one of the three elements in $\{y, yx, yx^2\}$. Also, we cannot have $xy = y$ since that implies that $x = 1$, which is not true. If $xy = yx^2$, we see that the group is just the dihedral group D_3. (We have already written out the multiplication table for this group in the lectures.)

Suppose $xy = yx$. Then,

$$(xy)^2 = xyxy = x(xy)y = x^2y^2 = x^2.$$

$$(xy)^3 = (xy)^2(xy) = x^2(xy) = y.$$

$$(xy)^4 = (xy)(xy)^3 = (xy)y = x.$$

$$(xy)^5 = (xy)(xy)^4 = (xy)x = (yx)x = yx^2.$$

Thus, we see that $ord(xy) = 6$. However, we are considering the case that there is no element of order 6. So we may discard this possibility.

Case 3: Any non-identity element of G has order 2.

Let x be a non-identity element. Then $ord(x) = 2$, and so $\langle x \rangle$ has 2 elements. Thus, there exists an element y such that $y \notin \langle x \rangle$. Then, we consider the four elements $\{1, x, y, yx\}$. Since every element is of order 2, $x^{-1} = x$, $y^{-1} = y$ and $(yx)^{-1} = yx$. However, $(yx)^{-1} = x^{-1}y^{-1} = xy$. Thus, we see that $xy = yx$. Now, we observe that the set $S = \{1, x, y, yx\}$ is actually closed under the binary operation and also under inverses. Thus, S is a subgroup of order 4. However, we know that the order of a subgroup has to divide the order of a group. (Here, I am using a theorem that was proved much after Tutorial 2, but you may actually imitate the arguments from earlier lecture to see that G cannot have a subgroup of order 4.) Thus, Case 3 cannot occur.

Groups of order 7: In this case, any non-identity element has order 7. So, any such group will isomorphic to the group of rotational symmetries of a regular heptagon. □

Problem 2. Compute the order of all elements in the dihedral group D_6. Can you do this for D_n?

Solution. The group D_6 is generated by the rotation through $2\pi/6$ radians, and a reflection τ. The following table gives the orders of all the elements:

1	ρ	ρ^2	ρ^3	ρ^4	ρ^5	τ	$\rho\tau$	$\rho^2\tau$	$\rho^3\tau$	$\rho^4\tau$	$\rho^5\tau$
1	6	3	2	3	6	2	2	2	2	2	2

In general, for any positive integer n, the group D_n is generated by the rotation through $2\pi/n$ radians, which we denote by ρ, and a reflection τ. The group has n rotations of the form ρ^i where $0 \leqslant i \leqslant n-1$. It can be proved that the order of the element ρ^i is $n/gcd(i, n)$. (We will prove this in a later lecture. But you may do so yourself.) There are also n reflections of the form $\rho^i\tau$ where $0 \leqslant i \leqslant n-1$, each of which has order 2. □

Problem 3. List all subgroups of D_6.

Solution. As above, let ρ denote the rotation through $2\pi/6$ radians and τ be a reflection. Then, we first consider the subgroups that are contained in $\langle \rho \rangle$. These are given as follows:

$$\langle 1 \rangle = \{1\}$$
$$\langle \rho \rangle = \{1, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}$$
$$\langle \rho^2 \rangle = \{1, \rho^2, \rho^4\}$$
$$\langle \rho^3 \rangle = \{1, \rho^3\}$$

(There are no other subgroups that are contained in $\langle \rho \rangle$. This fact needs to be proved and you can write a detailed proof by a case-by-case approach. However, we will look at cyclic groups in detail in a later lecture.)

Suppose H is a subgroup of D_6 which is not contained in $\langle \rho \rangle$. Then, the set $K = H \cap \langle \rho \rangle$ is a subgroup of ρ. (See the solution to Problem 4, which shows that the intersection of two subgroups is a subgroup.) Thus, K must be one of the four groups listed above. Let L denote the set of reflections in H. Thus, $H = K \cup L$ and $K \cap L = \varnothing$. Let τ_1 be any element of L. Then, the set $\tau_1 K$ is contained in L since the product of a reflection and a rotation is a reflection. Similarly, the set $\tau_1 L$ is contained in K since the product of two reflections is a rotation. Also, $|\tau_1 K| = |K|$ (see Lecture 7) and $|\tau_1 L| = |L|$. As $\tau_1 K \subset L$, we see that $|L| \geqslant |\tau_1 K| = |K|$.

Similarly, as $\tau_1 L \subset K$, we see that $|K| \geqslant |\tau_1 L| = |L|$. Thus, $|K| = |L|$ and we also have the equalities $\tau_1 K = L$ and $\tau_1 L = K$. Thus, $H = K \cup \tau_1 K$.

When $K = \langle 1 \rangle$, we may take τ_1 to be any of the 6 reflections of the form $\rho^i \tau$ where $0 \leqslant i \leqslant 5$. For each choice of τ_1, we find that $K \cup \tau_1 K$ is a group of order 2. Thus, we get 6 subgroups of the form

$$\langle \rho^i \tau \rangle = \{1, \rho^i \tau\}.$$

When $K = \langle \rho \rangle$, for any choice of τ_1, the set $K \cup \tau_1 K$ is equal to the whole group D_6. Thus, in this case, we get one group of order 12.

When $K = \langle \rho^2 \rangle$, we find that taking τ_1 to be τ, $\rho^2\tau$ or $\rho^4\tau$ gives the same set $H_1 = K \cup \tau_1 K$. In this case,

$$H_1 = \{1, \rho^2, \rho^4, \tau, \rho^2\tau, \rho^4\tau\}$$

and one can easily check that this is a subgroup.

Similarly, taking τ_1 to be $\rho\tau$, $rho^3\tau$ or $\rho^5\tau$ gives rise the same subgroup of D_6, which is

$$H_2 = \{1, \rho^2, \rho^4, \rho\tau, \rho^3\tau, \rho^5\tau\}.$$

Finally, taking $\langle K \rangle = \langle \rho^3 \rangle$, we find that we can get the following 3 subgroups of order 4:

$$\{1, \rho^3, \tau, \rho^3\tau\}$$
$$\{1, \rho^3, \rho\tau, \rho^4\tau\}$$
$$\{1, \rho^3, \rho^2\tau, \rho^5\tau\}$$

(You have to explicitly check that these are actually subgroups.) □

Problem 4. Let G be a group. Let H_1 and H_2 be subgroups of G. Is $H_1 \cap H_2$ (the intersection of H_1 and H_2) a subgroup of G? What about the union $H_1 \cup H_2$?

Solution. It is true that $H_1 \cap H_2$ is a subgroup if H_1 and H_2 are subgroups. To prove this, we have to check various conditions.

First we see that $1_G \in H_1$ and $1_G \in H_2$. Thus, $1_G \in H_1 \cap H_2$.

Suppose $x, y \in H_1 \cap H_2$. Then, $x, y \in H_1$ and so $xy \in H_1$ since H_1 is subgroup. Similarly, $x, y \in H_2$ and so $xy \in H_2$ since H_2 is a subgroup. Thus, $xy \in H_1 \cap H_2$.

Suppose $x \in H_1 \cap H_2$. Then $x \in H_1$ implies that $x^{-1} \in H_1$ as H_1 is a subgroup. Similarly, $x \in H_2$ implies that $x^{-1} \in H_2$ as H_2 is a subgroup. Thus, $x^{-1} \in H_1 \cap H_2$.

Thus, we see that $H_1 \cap H_2$ is a subgroup of G.

In general, if H_1 and H_2 are subgroups of G, the union $H_1 \cup H_2$ is not a subgroup of G. For example, in the group D_6, the sets $H_1 = \{1, \tau\}$ and $H_2 = \{1, \rho\tau\}$ are subgroups, but their union is not a subgroup. □

Problem 5. Let $\mathbb{Q}^\times$ denote the group of non-zero rational numbers under multiplication. Prove that the set of all numbers of the form $3^m 5^n$, where m and n are integers, is a subgroup of $\mathbb{Q}^\times$.

Proof. Let H denote the set of numbers of the form $3^m 5^n$ where m and n are integers.

Then, $1 = 3^0 \cdot 5^0$. Thus, $1 \in H$.

If $x = 3^a 5^b$ and $y = 3^c 5^d$. Then $xy = 3^{a+c} 5^{b+d}$, which is clearly in H.

Finally, if $x = 3^a 5^b$, then $x^{-1} = 3^{-a} 5^{-b}$ which is also in H.

This proves that H is a subgroup of $\mathbb{Q}^\times$. □