Math 304 Assignment 6 - Solutions

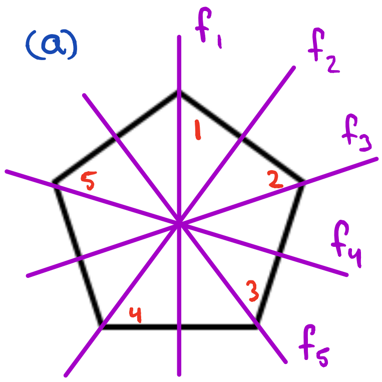
1. (a) $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(b) $U(10) = \{1,3,7,9\}$

$\bullet$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

2. (a)



Let 1 denote the "do nothing" symmetry.

Let r denote a rotation of $360/5 = 72°$ in the clockwise (cw) direction.

Then r^2 denotes a rotation of 144° cw,
and r^3 " " " " 216° cw,
and r^4 " " " " 288 cw.

For each $1 \le i \le 5$, f_i denotes the corresponding reflection across the axis drawn in the diagram.

There are 10 symmetries in all: $D_5 = \{1, r, r^2, r^3, r^4, f_1, f_2, f_3, f_4, f_5\}$
Each symmetry could also be represented by the permutation it induces on the labels on the vertices.

$1 \mapsto \varepsilon$ $\qquad f_1 \mapsto (25)(34)$

$r \mapsto (12345)$ $\qquad f_2 \mapsto (12)(35)$

$r^2 \mapsto (13524)$ $\qquad f_3 \mapsto (13)(45)$

$r^3 \mapsto (14253)$ $\qquad f_4 \mapsto (14)(23)$

$r^4 \mapsto (15432)$ $\qquad f_5 \mapsto (15)(24)$

(b)(c) Cayley table

	1	r	r^2	r^3	r^4	f_1	f_2	f_3	f_4	f_5
1	1	r	r^2	r^3	r^4	f_1	f_2	f_3	f_4	f_5
r	r	r^2	r^3	r^4	1	f_5	f_1	f_2	f_3	f_4
r^2	r^2	r^3	r^4	1	r	f_4	f_5	f_1	f_2	f_3
r^3	r^3	r^4	1	r	r^2	f_3	f_4	f_5	f_1	f_2
r^4	r^4	1	r	r^2	r^3	f_2	f_3	f_4	f_5	f_1
f_1	f_1	f_2	f_3	f_4	f_5	1	r	r^2	r^3	r^4
f_2	f_2	f_3	f_4	f_5	f_1	r^4	1	r	r^2	r^3
f_3	f_3	f_4	f_5	f_1	f_2	r^3	r^4	1	r	r^2
f_4	f_4	f_5	f_1	f_2	f_3	r^2	r^3	r^4	1	r
f_5	f_5	f_1	f_2	f_3	f_4	r	r^2	r^3	r^4	1

D_5 is not abelian since, for example, $rf_1 \neq f_1 r$.

(d) Since $|D_5| = 10$ it can only have subgroups of orders $1, 2, 5, 10$. The subgroup of order 1 is $\{1\}$, and the subgroup of order 10 is D_5 itself.

Subgroups of order 2: There are 5 of them, each corresponding to an element of order 2:

$$\langle f_1 \rangle, \langle f_2 \rangle, \langle f_3 \rangle, \langle f_4 \rangle, \langle f_5 \rangle.$$

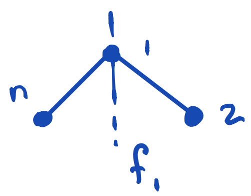
Subgroups of order 5: First observe that, by Corollary 11.1.5, every non-identity element in a subgroup of order 5 must have order 5 too. This means none of the reflections can be in a subgroup of order 5. The only subgroup of order 5 is

$$\langle r \rangle = \{1, r, r^2, r^3, r^4\}.$$

3. D_n is not cyclic. To see why we will provide a few different arguments.

Reason 1: There is no element of order $2n$. The rotations have order at most n (since they form a subgroup of size n), and the reflections each have order 2.

Reason 2: D_n is not abelian.



For example, consider reflection f_1 as drawn left, and rotation r. Then

$f_1 r$ takes vertex 1 to 2

but

$r f_1$ takes vertex 1 to n.

Therefore,

$$f_1 r \neq r f_1.$$

Since D_n is not abelian it cannot be cyclic.

Reason 3: D_n has at least n elements of order 2, namely the reflections. However, a cyclic group can have at most 1 element of order 2 (Theorem 11.5.3).

4. By Theorem 11.5.4(a) the generators of $\mathbb{Z}_{22}$ are: 1, 3, 5, 7, 9, 13, 15, 17, 19, 21

Notice there are $\varphi(22) = 10$ generators.

5. By Theorem 11.5.4(c) the elements of order 6 are

$$k \cdot 100 \quad \text{where } \gcd(k, 6) = 1.$$

There are 2 elements:

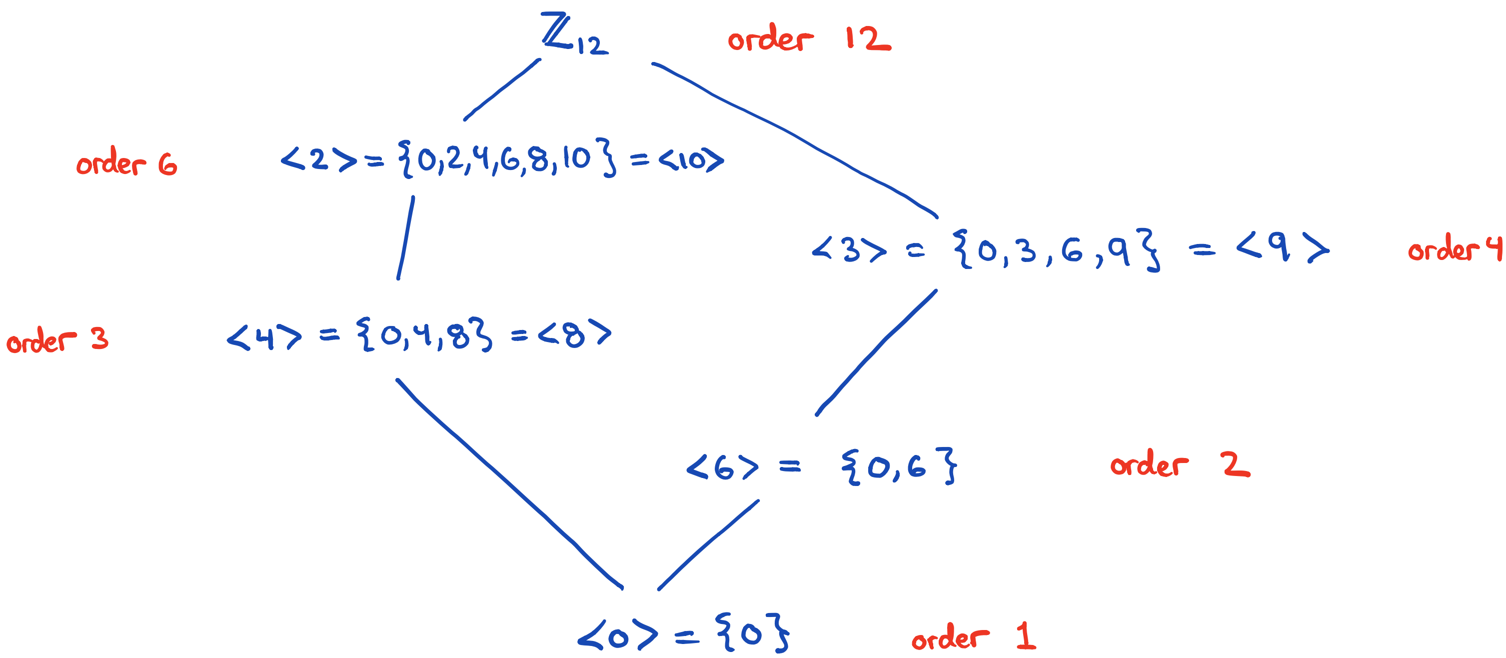
$$100, \quad 500$$

6. We'll use Theorem 11.5.4 (b) to find the subgroups and for each subgroup we use Theorem 11.9 (a) to get all generators.

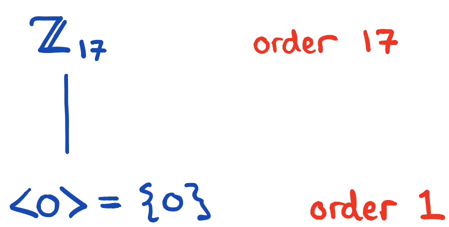
(a) $\mathbb{Z}_{12}$: The subgroups of $\mathbb{Z}_{12}$ are of sizes $1,2,3,4,6,12$.

order 12 subgroup : $\mathbb{Z}_{12} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$
order 6 subgroup : $\langle 2 \rangle = \{0,2,4,6,8,10\} = \langle 10 \rangle$
order 4 subgroup : $\langle 3 \rangle = \{0,3,6,9\} = \langle 9 \rangle$
order 3 subgroup : $\langle 4 \rangle = \{0,4,8\} = \langle 8 \rangle$
order 2 subgroup : $\langle 6 \rangle = \{0,6\}$
order 1 subgroup : $\langle 0 \rangle = \{0\}$

We can express this in the following diagram (graph):



(b) In $\mathbb{Z}_{17}$ the order of a subgroup divides 17, so it is either 17 (i.e. the whole group) or 1 (i.e. the trivial subgroup.



7. (a) $\langle (1\,2\,3\,4) \rangle = \{\varepsilon, (1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2)\} < S_4$ has order 4.

(b) $D_4 < S_4$ of order 8, where we view the elements of D_4 as permutations of the vertices of a square under the 8 symmetries.

8. G has $\varphi(10) = 4$ elements of order 10 by Theorem 11.5.3. If a is one element of order 10, then

$$a \, , \, a^3 \, , \, a^7 \, , \, a^9$$

are all the elements of order 10. Note: $1, 3, 7, 9$ are precisely the numbers less than, and relatively prime, to 10.

9. Since the order of an element divides the order of the group then any nonidentity element must have order p. Since $|G| = p$ then any nonidentity element generates the group. Therefore G is cyclic.

10. Let G be a group with the property that the square of every element is the identity. Let $g, h \in G$ be any two elements. Then

$$\begin{aligned} (gh)^2 &= e \quad , \text{ by the property of this group} \\ ghgh &= e \\ ghg &= h^{-1} \\ gh &= h^{-1}g^{-1} \\ gh &= hg \quad , \text{ since } h^2 = e = g^2 \text{ then } h^{-1} = h, \, g^{-1} = g \end{aligned}$$

Therefore G is abelian.

8. If $|G| = 33$ then the possible orders of elements are $1, 3, 11$ and 33.
Towards a contradiction suppose G does not have an element of order 3. Then it also can't have an element of order 33 (if g has order 33 then g^{11} has order 3). Therefore, under this assumption the elements of G have order either 1 or 11. There is only one element of order 1, namely the identity. There would then need to be 32 elements of order 11. We'll show that this is impossible.

First I'll give a quick argument as to why this is impossible. Afterwards, I'll give a more constructive argument. Consider

$$(*) \qquad \{ x \in G \mid x^{11} = e \text{ and } x \neq e \}$$

Since every element in G is assumed to have order 11 (or 1), then this set is $G \setminus \{e\}$ and must have 32 elements. However, for each element b of order 11 it has 10 related elements:

$$b, b^2, b^3, \ldots, b^9, b^{10}$$

all of which have order 11. Therefore, $(*)$ can be split up into disjoint sets of size 10, which means its cardinality is divisible by 10. But $10 \nmid 32$, so we have a contradiction.

We've seen this argument before (assignment 2 #13)

The following is a more constructive argument showing that all non-identity elements cannot have order 11.

Consider an element of order 11, say a. Then

$$\langle a\rangle = \{e, a, a^2, \dots, a^{10}\}$$

Pick another element in G that is not in $\langle a\rangle$, call this b. Then b has order 11 and

$$\langle b\rangle = \{e, b, b^2, \dots, b^{10}\}$$

<u>Claim</u>: $\langle a\rangle \cap \langle b\rangle = \{e\}$

Pf: If $x \in \langle a\rangle \cap \langle b\rangle$ s.t. $x = e$ then x has order 11 so $\langle a\rangle = \langle x\rangle = \langle b\rangle$
$\rightarrow\leftarrow$ $\square$

Now $\langle a\rangle \cup \langle b\rangle$ consists of 21 elements of G (identity common to both).
Let $c \in G \setminus (\langle a\rangle \cup \langle b\rangle)$, and by a similar argument

$$\langle a\rangle, \langle b\rangle, \langle c\rangle$$

only share the identity element. Together they consist of 31 elements of G. So there is still another element

$$d \in G \setminus (\langle a\rangle \cup \langle b\rangle \cup \langle c\rangle)$$

which has order 11. But
$$\langle d\rangle = \{e, d, d^2, \dots, d^{10}\}$$
would consist of 10 elements in G which are not in $\langle a\rangle \cup \langle b\rangle \cup \langle c\rangle$. This is impossible since it would imply $|G| \geq 41$.

Therefore, G must have an element of order 3.

$\square$