PMATH 336 Intro to Group Theory, Solutions to Assignment 2

1: Sketch a picture of each of the following subsets of $\mathbb{C}^*$ and, in parts (c) and (d), determine whether the given subset is a subgroup (under multiplication).

(a) $\left\langle \frac{i-1}{\sqrt{2}} \right\rangle$

Solution: Let $\alpha = \frac{i-1}{\sqrt{2}} = e^{i\,3\pi/4}$. Then $\alpha^2 = e^{i\,6\pi/4} = e^{-i\,\pi/2}$, $\alpha^3 = e^{i\,9\pi/4} = e^{i\,\pi/4}$, $\alpha^4 = e^{i\,12\pi/4} = e^{i\,\pi}$, $\alpha^5 = e^{i\,15\pi/4} = e^{-i\,\pi/4}$, $\alpha^6 = e^{i\,18\pi/4} = e^{i\pi/2}$, $\alpha^7 = e^{i\,21\pi/4} = e^{-i\,3\pi/4}$ and $\alpha^8 = e^{i\,24\pi/4} = e^{i\,0}$, and then $\alpha^9 = \alpha$ again, and so $\langle\alpha\rangle$ is the set of 8^{th} roots of 1 in $\mathbb{C}^*$. These are shown below in red.

(b) $\langle 1+i \rangle$

Solution: Let $\beta = 1+i$. A few of the positive powers of β are $\beta^2 = 2i$, $\beta^3 = -2+2i$, $\beta^4 = -4$ and $\beta^5 = -4-4i$, and a few of the negative powers of β are $\beta^{-1} = \frac{1}{2} - \frac{1}{2}\,i$, $\beta^{-2} = -\frac{1}{2}\,i$, $\beta^{-3} = -\frac{1}{4} - \frac{1}{4}\,i$, $\beta^{-4} = -\frac{1}{4}$ and $\beta^{-5} = -\frac{1}{8} - \frac{1}{8}i$. These are shown below in blue.

(c) $\left\{ z \in \mathbb{C}^* \middle| \, z^8 = |z|^8 \right\}$ (where $|z|$ denotes the usual norm of z)

Solution: Write $H = \{z \in \mathbb{C}^* |\, z^8 = |z|^8\}$. We show that H is a subgroup of $\mathbb{C}^*$.
Closure: $z, w \in H \Longrightarrow z^8 = |z|^8$ and $w^8 = |w|^8 \Longrightarrow (zw)^8 = z^8 w^8 = |z||^8|w||^8 = |zw|^8 \Longrightarrow zw \in H$.
Identity: $1 \in H$ since $1^8 = |1|^8$.
Inverse: $z \in H \Longrightarrow z^8 = |z|^8 \Longrightarrow \left(\frac{1}{z}\right)^8 = \frac{1}{z^8} = \frac{1}{|z|^8} = \left|\frac{1}{z}\right|^8 \Longrightarrow \frac{1}{z} \in H$.

To sketch a picture of this group H, note that for $z = r\,e^{i\theta}$ we have $z^8 = |z|^8 \iff r^8 e^{i\,8\theta} = r^8 \iff e^{i\,8\theta} = 1 \iff 8\theta = 2\pi\,k$ for some integer $k \iff \theta = \frac{\pi}{4}\,k$ for some k. Thus H is the union of the lines $y=0$, $y=x$, $x=0$ and $y=-x$, shown below in peach.

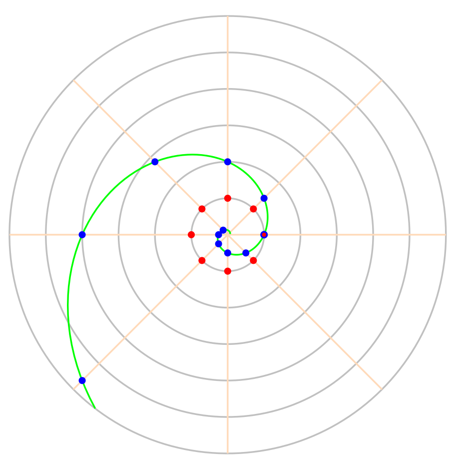
(d) $\left\{ re^{i\,\theta} \in \mathbb{C}^* \middle| \, r > 0\,,\, \theta = \frac{\pi}{2}\log_2 r \right\}$.

Solution: Let $K = \{re^{i\theta} \in \mathbb{C}^* |\, \theta = \frac{\pi}{2}\log_2(r)\} = \{re^{i\theta} \in \mathbb{C}^* |\, r = 2^{2\theta/\pi}\}$. Then K is a subgroup of $\mathbb{C}^*$:
Closure: if $r\,e^{i\alpha}$ and $s\,e^{i\beta}$ are both in K, then $r = 2^{2\alpha/\pi}$ and $s = 2^{2\beta/\pi}$ and so

$$(r\,e^{i\alpha})(s\,e^{i\beta}) = rs\,e^{i(\alpha+\beta)} = 2^{2\alpha/\pi}\,2^{2\beta/\pi}\,e^{i(\alpha+\beta)} = 2^{2(\alpha+\beta)/\pi}e^{i(\alpha+\beta)} \in K\,.$$

Identity: We have $1 = r\,e^{i\theta}$ when $r=1$ and $\theta=0$, and then $r = 1 = 2^0 = 2^{2\theta/\pi}$, and so $1 \in K$.
Inverse: $z = r\,e^{i\theta} \in K \Longrightarrow r = 2^{2\theta/2} \Longrightarrow r^{-1} = 2^{-2\theta/\pi} \Longrightarrow r^{-1}e^{-i\theta} \in K \Longrightarrow z^{-1} \in K$.

This group may be sketched by plotting points (r,θ) with $r = 2^{2\theta/\pi}$ on a polar grid. It is shown below in green.



2: Consider the group $D_6 = \{I, R_1, R_2, R_3, R_4, R_5, F_0, F_1, F_2, F_3, F_4, F_5\}$.

(a) Make the multiplication table for D_6.

Solution: Here is the multiplication table.

$A \backslash B$	I	R_1	R_2	R_3	R_4	R_5	F_0	F_1	F_2	F_3	F_4	F_5
I	I	R_1	R_2	R_3	R_4	R_5	F_0	F_1	F_2	F_3	F_4	F_5
R_1	R_1	R_2	R_3	R_4	R_5	I	F_1	F_2	F_3	F_4	F_5	F_0
R_2	R_2	R_3	R_4	R_5	I	R_1	F_2	F_3	F_4	F_5	F_0	F_1
R_3	R_3	R_4	R_5	I	R_1	R_2	F_3	F_4	F_5	F_0	F_1	F_2
R_4	R_4	R_5	I	R_1	R_2	R_3	F_4	F_5	F_0	F_1	F_2	F_3
R_5	R_5	I	R_1	R_2	R_3	R_4	F_5	F_0	F_1	F_2	F_3	F_4
F_0	F_0	F_5	F_4	F_3	F_2	F_1	I	R_5	R_4	R_3	R_2	R_1
F_1	F_1	F_0	F_5	F_4	F_3	F_2	R_1	I	R_5	R_4	R_3	R_2
F_2	F_2	F_1	F_0	F_5	F_4	F_3	R_2	R_1	I	R_5	R_4	R_3
F_3	F_3	F_2	F_1	F_0	F_5	F_4	R_3	R_2	R_1	I	R_5	R_4
F_4	F_4	F_3	F_2	F_1	F_0	F_5	R_4	R_3	R_2	$R1$	I	R_5
F_5	F_5	F_4	F_3	F_2	F_1	F_0	R_5	R_4	R_3	R_2	R_1	I

(b) Find the order of each element in D_6.

Solution: For each index $k \in \mathbb{Z}_6$, we have $F_k \neq I$ and ${f_k}^2 = I$ and so $|F_k| = 2$. Since $|R_1| = 6$ and $R_k = (R_1)^6$ we have $|R_k| = \frac{6}{\gcd(k,6)}$ for all indices k. To be explicit, we have

A	I	R_1	R_2	R_3	R_4	R_5	F_0	F_1	F_2	F_3	F_4	F_5
$\lvert A\rvert$	1	6	3	2	3	6	2	2	2	2	2	2

(c) Solve the equation $X^2Y^3 = R_1$ for X and Y in D_6.

Solution: We have the following table of powers.

X	I	R_1	R_2	R_3	R_4	R_5	F_0	F_1	F_2	F_3	F_4	F_5
X^2	I	R_2	R_4	I	R_2	R_4	I	I	I	I	I	I
X^3	I	R_3	I	R_3	I	R_3	F_0	F_1	F_2	F_3	F_4	F_5

From the table of powers, we see that X^2 is equal to I, R_2 or R_4. When $X^2 = I$ we have $X^2Y^3 = R_1 \iff Y^3 = R_1$, but there is no element $Y \in D_6$ with $Y^3 = R_1$, so there is no solution with $X^2 = I$. When $X^2 = R_2$ we have $X^2Y^3 = R_1 \iff R_2Y^3 = R_1 \iff R_4R_2Y^3 = R_4R_1 \iff Y^3 = R_5$, but there is no element $Y \in D_6$ with $Y^3 = R_5$. Finally, when $X^2 = R_4$ (that is when $X \in \{R_2, R_5\}$) we have $X^2Y^3 = R_1 \iff R_4Y^3 = R_1 \iff R_2R_4Y^3 = R_2R_1 \iff Y^3 = R_3 \iff Y \in \{R_1, R_3, R_5\}$. Thus the solutions are $(X, Y) = (R_2, R_1)$, (R_2, R_3), (R_2, R_5), (R_5, R_1), (R_5, R_3) and (R_5, R_5).

3: (a) Show that U_{25} is cyclic.

Solution: We have $U_{25} = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$. We make a table of powers of 2 modulo 25.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2^k	1	2	4	8	16	7	14	3	6	12	24	23	21	17	9	18	11	22	19	13	1

We see that $U_{25} = \langle 2 \rangle$, so it is cyclic.

(b) List all the elements and all the generators of every subgroup of U_{25}.

Solution: The divisors of 20 are $1, 2, 4, 5, 10, 20$ so the subgroups of U_{25} are

$$\begin{aligned}
\langle 2^1 \rangle &= U_{25} \\
\langle 2^2 \rangle &= \left\{2^0, 2^2, 2^4, 2^6, 2^8, 2^{10}, 2^{12}, 2^{14}, 2^{16}, 2^{18}\right\} = \left\{1, 4, 16, 14, 6, 24, 21, 9, 11, 19\right\} \\
\langle 2^4 \rangle &= \left\{2^0, 2^4, 2^8, 2^{12}, 2^{16}\right\} = \left\{1, 16, 6, 21, 11\right\} \\
\langle 2^5 \rangle &= \left\{2^0, 2^5, 2^{10}, 2^{15}\right\} = \left\{1, 7, 24, 18\right\} \\
\langle 2^{10} \rangle &= \left\{2^0, 2^{10}\right\} = \left\{1, 24\right\} \\
\langle 2^{20} \rangle &= \left\{2^0\right\} = \left\{1\right\}
\end{aligned}$$

Since $|2^1| = 20$ and we have $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$, the set of generators of the subgroup $\langle 2^1 \rangle$ is $\left\{2^1, 2^3, 2^7, 2^9, 2^{11}, 2^{13}, 2^{17}, 2^{19}\right\} = \left\{2, 8, 3, 12, 23, 17, 22, 13\right\}$. Since $|2^2| = 10$ and $U_{10} = \{1, 3, 7, 9\}$, the set of generators of $\langle 2^2 \rangle$ is $\left\{2^2, 2^6, 2^{14}, 2^{18}\right\} = \{4, 14, 9, 19\}$. Since $|2^4| = 5$ and $U_5 = \{1, 2, 3, 4\}$, the set of generators of $\langle 2^4 \rangle$ is $\left\{2^4, 2^8, 2^{12}, 2^{16}\right\} = \{16, 6, 21, 11\}$. Since $|2^5| = 4$ and $U_4 = \{1, 3\}$, the set of generators of $\langle 2^5 \rangle$ is $\left\{2^5, 2^{15}\right\} = \{7, 18\}$. The only generator of $\langle 2^{10} \rangle$ is $2^{10} = 24$. The only generator of $\langle 2^{20} \rangle$ is $2^0 = 1$.

(c) Find a non-cyclic subgroup of order 4 in U_{20}.

Solution: We have $U_{20} = \left\{1, 3, 7, 9, 11, 13, 17, 19\right\}$. We make a table of powers modulo 20 and determine the order of each element.

x	1	3	7	9	11	13	17	19
x^2	1	9	9	1	1	9	9	1
x^3	1	7	3	9	11	17	13	19
x^4	1	1	1	1	1	1	1	1
$\|x\|$	1	4	4	2	2	4	4	2

A non-cyclic subgroup of order 4 cannot have any elements of order 4, so the only possible non-cyclic subgroup is $H = \{1, 9, 11, 19\}$. To verify that this subset H is a subgroup, it is enough to show that H is closed under multiplication, and indeed we have $9 \cdot 11 = 19$, $9 \cdot 19 = 11$ and $11 \cdot 19 = 9$.

4: Let G be a multiplicative group and let $a \in G$ with $|a| = 1400$.

(a) Determine the number of subgroups of $\langle a \rangle$.

Solution: We have $a = 2^3 5^2 7^1$. The divisors of a are of the form $2^i 5^j 7^k$ with $0 \le i \le 3$, $0 \le j \le 2$ and $0 \le k \le 1$. Since there are 4 choices for i, 3 for j and 2 for k, we see that a has $4 \cdot 3 \cdot 2 = 24$ divisors. Thus the cyclic group $\langle a \rangle$ has 24 subgroups.

(b) Determine the number of elements $x \in \langle a \rangle$ with $|x| \le 10$.

Solution: The divisors of 1400 which are at most 10 are 1, 2, 4, 5, 7, 8, 10, so the number of elements $x \in \langle a \rangle$ with $|x| \le 10$ is equal to $\phi(1) + \phi(2) + \phi(4) + \phi(5) + \phi(7) + \phi(8) + \phi(10) = 1 + 1 + 2 + 4 + 6 + 4 + 4 = 22$.

(c) List all the elements $x = a^k \in \langle a \rangle$ with $x^{52} = 1$.

Solution: For $x = a^k$ we have

$$x^{52} = e \iff a^{52\,k} = a^0 \iff 52\,k = 0 \ (\text{ mod } 1400) \iff 13\,k = 0 \ (\text{ mod } 350) \iff k = 0 \ (\text{ mod } 350)$$
$$\iff k \in \{0, 350, 700, 1050\} \iff x \in \left\{e, a^{350}, a^{700}, a^{1050}\right\}$$

(d) Find the number of pairs (x, y) with $x, y \in \langle a \rangle$ such that $x^{10} = y^{35}$ in $\langle a \rangle$.

Solution: Let $x, y \in \langle a \rangle$, say $x = a^k$ and $y = a^\ell$ where $0 \le k, \ell < 1400$. We have

$$x^{10} = y^{35} \iff a^{10k} = a^{35\ell} \iff 10k = 35\ell \text{ mod } 1400 \iff 2k = 7\ell \text{ mod } 280$$
$$\iff \ell \text{ is even and } k = \tfrac{7\ell}{2} \text{ mod } 140.$$

For each of the 700 even choices for ℓ, there is a unique value of k modulo 140, so there are 10 choices for k modulo 1400. Thus there are $700 \cdot 10 = 7000$ such pairs (x, y).