PMATH 336 Intro to Group Theory, Solutions to Assignment 4

1: (a) Let $G = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in GL_2(\mathbb{R}) \,\middle|\, a, b \in \mathbb{R} \right\}$. Show that G is a group and that $G \cong \mathbb{C}^*$.

Solution: First we show that G is a group. G is closed under matrix multiplication since if $A, B \in G$, say $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ and $B = \begin{pmatrix} c & -d \\ d & c \end{pmatrix}$, then $AB = \begin{pmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{pmatrix}$, which is of the correct form to belong to G, and since A and B are invertible, we know (from linear algebra) that AB is also invertible, hence $AB \in G$. Also, we clearly have $I \in G$. Finally, if $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in G$ then A is invertible with $A^{-1} = \frac{1}{a^2+b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, so $A^{-1} \in G$.

Now we show that $G \cong \mathbb{C}^*$. Define $\phi : G \to \mathbb{C}^*$ by $\phi\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a + i\,b$. This map ϕ is well defined since when $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in G$ we have $\det A = a^2 + b^2 \neq 0$ and so $a + i\,b \neq 0$ and so $a + i\,b \in \mathbb{C}^*$. ϕ is onto since given $z = a + i\,b \in \mathbb{C}^*$ we can let $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ and then $\det A = a^2 + b^2 \neq 0$ so $A \in G$ and we have $\phi(A) = z$. The map ϕ is clearly one-to-one. Finally, ϕ preserves the operations since

$$\begin{aligned} \phi\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix}\right) &= \phi\begin{pmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{pmatrix} = (ac - bd) + i(ad + bc) \\ &= (a + i\,b)(c + i\,d) = \phi\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\phi\begin{pmatrix} c & -d \\ d & c \end{pmatrix}. \end{aligned}$$

(b) Suppose that $\phi : U_{30} \to \mathbb{Z}_2 \times \mathbb{Z}_4$ is a group isomorphism. Find $\phi(19)$.

Solution: In U_{30} note that $7^2 = 19$, $7^3 = 13$ and $7^4 = 1$ so that $|7| = 4$. Since ϕ is an isomorphism we must have $\left|\phi(7)\right| = 4$ and so $\phi(7) \in \left\{(0,1), (1,1), (0,3), (1,3)\right\}$. Thus $\phi(19) = \phi(7^2) = 2\phi(7) = (0,2)$.

2: Show that no two of the groups $\mathbb{Z}_{12}$, U_{28}, D_6 and A_4 are isomorphic.

Solution: The number of elements of each order in $\mathbb{Z}_{12}$ is given by

$\lvert a\rvert$	1	2	3	4	6	12
# of such a	1	1	2	2	2	4

In $U_{28} = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}$ we have

k	0	1	2	3	4	5	6
3^k	1	3	9	27	25	19	1
5^k	1	5	25	13	9	17	1
11^k	1	11	9	15	25	23	1

From the list of powers of 3 we see that $|3| = |19| = 6$, $|9| = |25| = 3$ and $|27| = 2$, from the list of powers of 5 we see that $|5| = |17| = 6$ and $|13| = 2$, and from the list of powers of 11 we see that $|11| = |23| = 6$ and $|15| = 2$, and so we have

x	1	3	5	9	11	13	15	17	19	23	25	27
$\lvert x\rvert$	1	6	6	3	6	2	2	6	6	6	3	2

Thus the number of elements of each order in U_{28} is given by

$\lvert x\rvert$	1	2	3	6
# of such x	1	3	2	6

The orders of the elements in D_6 are

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

so the number of elements of each order in D_6 is as follows

$\lvert A\rvert$	1	2	3	6
# of such A	1	7	2	2

Finally, in A_4 we have

form of α	$\lvert\alpha\rvert$	# of such α
(abc)	3	8
$(ab)(cd)$	2	3
(a)	1	1

We see that no two of the four given groups have the same number of elements of each order, and so no two of them are isomorphic.

3: (a) The elements of D_4 permute the 4^{th} roots of unity, namely $e^{i\,k\pi/2}$ for $k \in \mathbb{Z}_4 = \{1,2,3,4\}$, and so each element of D_4 determines a permutation of $\mathbb{Z}_4$. In this way, we can think of D_4 as a subgroup of S_4. To be precise, there is an isomorphism $\phi : D_4 \to H = \phi(D_4) \le S_4$ which is determined by $\phi(R_1) = (1234)$ and $\phi(F_0) = (13)$. Find all the elements of $H = \phi(D_4)$.

Solution: We have $\phi(1) = (1)$, $\phi(R_1) = (1234)$, $\phi(R_2) = \phi({R_1}^2) = \phi(R_1)^2 = (1234)^2 = (13)(24)$, $\phi(R_3) = \phi(R_1)^3 = (1234)^3 = (1432)$, $\phi(F_0) = (13)$, $\phi(F_1) = \phi(R_1F_0) = \phi(R_1)\phi(F_0) = (1234)(13) = (14)(23)$, $\phi(F_2) = \phi(R_2)\phi(F_0) = (13)(24)(13) = (24)$ and $\phi(F_3) = \phi(R_3)\phi(F_0) = (1432)(13) = (12)(34)$ (these values can also be seen geometrically), so $H = \phi(D_4) = \{(1), (1234), (13)(24), (1432), (13), (14)(23), (24), (12)(34)\}$.

(b) Let $f : U_9 \to \{1,2,3,4,5,6\}$ be the bijection given by

x	1	2	4	5	7	8
$f(x)$	1	2	3	4	5	6

and define $\phi : U_9 \to S_6$ by $\phi(a) = f \circ L_a \circ f^{-1}$, that is $\phi(a)(k) = f\big(a\,f^{-1}(k)\big)$. List all the elements in $\phi\big(U_9\big)$.

Solution: The following table shows $\phi(a)(k) = f(a\,f^{-1}(k))$ for the different values of a and k, so the permutation $\phi(a)$ appears in row a (for example we have $\phi(2)(5) = f(2\cdot f^{-1}(5)) = f(2\cdot 7) = f(14 \bmod 9) = f(5) = 4$).

a \ k	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	6	1	4	5
4	3	6	5	2	1	4
5	4	1	2	5	6	3
7	5	4	1	6	3	2
8	6	5	4	3	2	1

Thus $\phi(U_9) = \{(1), (123654), (135)(264), (145632), (153)(246), (16)(25)(34)\}$. (one way to check the answer is to notice that U_9 is cyclic with generator 2 and so $\phi(G)$ should be cyclic with generator $\phi(2) = (123654)$).

4: (a) Find $\text{Inn}(D_4)$ (that is, list all the distinct elements in $\text{Inn}(D_4)$).

Solution: Using the rules $R_kR_lR_{-k} = R_l$, $R_kF_lR_{-k} = R_kF_{l+k} = R_{2k+l}$, $F_kR_lF_k = F_kF_{k+l} = R_{-l}$ and $F_kF_lF_k = F_kR_{l-k} = F_{2k-l}$, we make a table showing the values of $\mathcal{C}_a(x) = a\,x\,a^{-1}$ for $a, x \in D_4$.

a\ x	I	R_1	R_2	R_3	F_0	F_1	F_2	F_3
I	I	R_1	R_2	R_3	F_0	F_1	F_2	F_3
R_1	I	R_1	R_2	R_3	F_2	F_3	F_0	F_1
R_2	I	R_1	R_2	R_3	F_0	F_1	F_2	F_3
R_3	I	R_1	R_2	R_3	F_2	F_3	F_0	F_1
F_0	I	R_3	R_2	R_1	F_0	F_3	F_2	F_1
F_1	I	R_3	R_2	R_1	F_2	F_1	F_0	F_3
F_2	I	R_3	R_2	R_1	F_0	F_3	F_2	F_1
F_3	I	R_3	R_2	R_1	F_2	F_1	F_0	F_3

We se that there are 4 distinct rows, indeed $I = \mathcal{C}_I = \mathcal{C}_{R_2}$, $\mathcal{C}_{R_1} = \mathcal{C}_{R_3}$, $\mathcal{C}_{F_0} = \mathcal{C}_{F_2}$ and $\mathcal{C}_{F_1} = \mathcal{C}_{F_3}$, so there are 4 distinct inner automorphisms; $\text{Inn}(D_4) = \{I, \mathcal{C}_{R_1}, \mathcal{C}_{F_0}, \mathcal{C}_{F_1}\}$.

(b) Show that $\big|\text{Aut}(D_4)\big| > \big|\text{Inn}(D_4)\big|$.

Solution: Since $\text{Inn}(D_4)$ is a subgroup of $\text{Aut}(D_4)$ we have $\big|\text{Aut}(D_4)\big| \ge \big|\text{Inn}(D_4)\big|$, so we must find one element of $\text{Aut}(D_4)$ which is not an element of $\text{Inn}(D_4)$. Define $\phi : D_4 \to D_4$ by $\phi(R_k) = R_k$ and $\phi(F_l) = F_{l+1}$. Then ϕ is clearly bijective. And ϕ preserves the operation since $\phi(R_kR_l) = \phi(R_{k+l}) = R_{k+l} = R_kR_l = \phi(R_k)\phi(R_l)$, $\phi(R_kF_l) = \phi(F_{k+l}) = F_{k+l+1} = R_kF_{l+1} = \phi(R_k)\phi(F_l)$, $\phi(F_kR_l) = \phi(F_{k-l}) = F_{k_l+1} = F_{k+1}R_l = \phi(F_k)\phi(R_l)$ and $\phi(F_kF_l) = \phi(R_{k-l}) = R_{k-l} = F_{k+1}F_{l+1} = \phi(F_k)\phi(F_l)$. Thus $\phi \in \text{Aut}(D_4)$. But, from the above table, there is no inner automorphism which maps F_0 to F_1, and so $\phi \notin \text{Inn}(D_4)$.