MA151 Algebra 1, Assignment 2

Dyson Dyson

Question 1

Let $A = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Show that A and B are elements of $GL_2(\mathbb{R})$ and determine their orders.

$\det A = \frac{1}{2} + \frac{1}{2} = 1$ and $\det B = 1 - 0 = 1$, so both A and B are non-singular 2×2 matrices with elements from $\mathbb{R}$, so they are both members of $\mathrm{GL}_2(R)$.

A is the matrix representing a rotation of 45° anticlockwise, so it has order 8. This can be checked by doing A^8 longhand, but I'm not going to do that.

B however, has infinite order, since $B^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, which I shall now prove by induction.

The base case of $n = 1$ is true, since $B^1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Now assume that $B^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ for some k. Then

$$B^{k+1} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+0 & 1+k \\ 0+0 & 0+1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 0 \end{pmatrix}$$

Therefore $B^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for all n. Therefore the only power of B that will give the identity is B^0, so B has infinite order.

Question 2

> Let G be a group and let $g \in G$. Suppose that $g^{12} = 1$ and let n be the order of g. What are the possibilities for n? Justify you answer.

The order of g could be any factor of 12. For instance, if $g^3 = 1$, then $g^{12} = \left(g^3\right)^4 = 1^4 = 1$. Therefore n could be any of $1, 2, 3, 4, 6, 12$.

Question 3

> In each of the following groups G, write down the cyclic subgroup generated by the given element $g \in G$. You don't need to justify your answers.

Q3 (a)

> $G = \mathbb{S} = \{z \in \mathbb{C} : |z| = 1\}, \quad g = e^{2\pi i/7}$

$\langle g \rangle = \left\{e^{2\pi i/7}, e^{4\pi i/7}, e^{6\pi i/7}, e^{8\pi i/7}, e^{10\pi i/7}, e^{12\pi i/7}, e^{12\pi i/7}, e^{12\pi i/7}\right\}$.

Q3 (b)

> $G = \mathrm{GL}_2(\mathbb{R}), \quad g = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

$\langle g \rangle = \left\{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$.

Q3 (c)

> $G = \mathrm{GL}_2(\mathbb{R}), \quad g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

$\langle g \rangle = \left\{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \dots\right\} = \left\{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : N \in \mathbb{N}, n \neq 0\right\}$.

Q3 (d)

> $G = D_8, \quad g = \rho_3$

$\langle g \rangle = \{\rho_3, \rho_2, \rho_1, \rho_0\}$.

Question 4

> Let R be the group of non-zero real numbers under multiplication. Let $H = \{x \in \mathbb{R} \mid x^2 \text{ is rational}\}$. Prove that H is a subgroup of $\mathbb{R}^*$.

We shall use the ABC test to show that H is a subgroup of $\mathbb{R}^*$.

The identity in $\mathbb{R}^*$ is the real number 1, whose square is rational, so 1 is also in H.

Suppose we have $a, b \in H$. That means $a^2, b^2 \in \mathbb{Q}$. Multiplying these gives ab, and since a^2 and b^2 are both rational, $(ab)^2 = a^2b^2$ is also rational, so ab is in H as well.

If we have some element $a \in H$, then $a^2 \in \mathbb{Q}$. The inverse of a in $\mathbb{R}^*$ is $\frac{1}{a}$, and $\left(\frac{1}{a}\right)^2 = \frac{1}{a^2}$ is also rational, therefore $a^{-1} \in H$.

Question 5

> Let G be a group and let $g \in G$. Show that g and g^{-1} have the same order.

Either g has finite order or g has infinite order.

In the case that g has finite order n, we know that $g^n = 1$. If we left-multiply both sides by g^{-n}, then we get $g^{-n}g^n = g^{-n}1 \implies 1 = g^{-n} = \left(g^{-1}\right)^n$. Therefore the order of g^{-1} must be a factor of n.

If the order of g^{-1} was some factor $k < n$, then $g^{-k} = 1$ and by the same logic, $g^kg^{-k} = g^k1 \implies 1 = g^k$, which would imply that the order of g is k, which is a contradiction. Therefore the order of g^{-1} must be n.

In the case that g has infinite order, we know that every power of g must be unique. And every power of g must have an inverse. Since inverses are unique, every power of g must have a unique inverse. Therefore $g \neq g^2 \neq g^3 \neq \cdots$ and $g^{-1} \neq g^{-2} \neq g^{-3} \neq \cdots$, therefore g^{-1} has infinite order.

Question 6

> Let G be a group and suppose $g \in G$ has infinite order. Show that G has infinitely many subgroups.

Every positive integer power of g generates a unique cyclic subgroup of infinite order. For example, we have the groups $\langle g^2 \rangle = \{\ldots, g^{-6}, g^{-4}, g^{-2}, 1, g^2, g^4, g^6, \ldots\}$, $\langle g^3 \rangle = \{\ldots, g^{-9}, g^{-6}, g^{-3}, 1, g^3, g^6, g^9, \ldots\}$. Since g has infinite order, there is no n such that $g^n = 1$, so all of these subgroups have infinite order, and all of them are unique.

The set of all such subgroups of G can be written as $\left\{ \{ g^{kn} \mid k \in \mathbb{Z} \} \;\middle|\; n \in \mathbb{Z} \right\}$.