Needham, Chapter 3, Exercise 20, pp. 186-7.
G. Palmer, August 26, 2021, 2:30 pm PDT

20. (i) Show that every Möbius transformation of the form

$$M(z) = \frac{pz+q}{\overline{q}z+\overline{p}} \qquad \textit{where } |p| > |q|$$

can be rewritten in the form

$$M(z) = e^{i\theta}\left(\frac{z-a}{\overline{a}z-1}\right), \textit{ where } |a| < 1$$

[Notice that the converse is also true. In other words, the two sets of functions are the same.]

Multiply through numerator and denominator by (1/p) so that z has coefficient 1 in the numerator.

$$\frac{pz+q}{\overline{q}z+\overline{p}} = \frac{z+q/p}{(\overline{q}/p)z+\overline{p}/p} \qquad\qquad (1)$$

Let $a = -q/p$, so $q/p = -a$ and $\overline{q} = -\overline{a}\,\overline{p}$. Substitute into (1) for q/p and $\overline{q}$.

$$\frac{z-a}{(-\overline{a}\,\overline{p}/p)z+\overline{p}/p} = \frac{z-a}{(-\overline{p}/p)(\overline{a}z-1)} = -\frac{p}{\overline{p}}\left(\frac{z-a}{\overline{a}z-1}\right)$$

Let $p = re^{i\phi}$

$$-\frac{p}{\overline{p}} = -\frac{re^{i\phi}}{re^{-i\phi}} = -e^{i2\phi} = e^{i(2\phi+\pi)}$$

Then $\frac{pz+q}{\overline{q}z+\overline{p}} = e^{i\theta}\,\frac{z-a}{(\overline{a}z-1)}$, where $\theta = 2\phi+\pi$

Note that $a = -\frac{q}{p}$; Then $|a| = \left|\frac{q}{p}\right| = \frac{|q|}{|p|}$, so if $|p| > |q|$, $|a| < 1$. I was reminded of this step by a message on Vasco's blog.

(ii) Use the matrix representation of the first equation to show that this set of Möbius transformations forms a group under the operation of composition.

Refer to pp. 156-7 for matrix representation. Refer to page 32 for group properties.

If the set of matrices corresponding to M is to form a group under composition, they must include an identity transformation, an inverse for every member, and compositions of members of M must have the same properties as those defining the set.

The matrix set corresponding to the given Möbius set M is written $[M] = \begin{bmatrix} p & q \\ \overline{q} & \overline{p} \end{bmatrix}$, which represents a set of matrices characterized by conjugate pairs on the diagonals and $|p| > |q|$.

The Identity Matrix:

The set [M] has an identity matrix $[\mathcal{E}] = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, so that [$\mathcal{E}$].[M] = [M]. The identity matrix has the same properties as [M]. It has diagonal conjugate pairs because the conjugates of real numbers are identities. |p| > |q| is satisfied by 1 > 0.

$$[\mathcal{E}].[\mathrm{M}] = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.\begin{bmatrix} p & q \\ \overline{q} & \overline{p} \end{bmatrix} = \begin{bmatrix} p & q \\ \overline{q} & \overline{p} \end{bmatrix}$$

The Inverse Matrix

[M] has an inverse, $[M]^{-1} = \frac{1}{\det([M])}\left[M^{-1}\right]$, such that $[M]^{-1}$.[M] = [$\mathcal{E}$], demonstrated as follows:

$$\left[M^{-1}\right] = \begin{bmatrix} \overline{p} & -q \\ -\overline{q} & p \end{bmatrix}$$

$$|\, p\,|^2 - |\, q\,|^2$$

$$\det([M]) = \overline{p}\mathrm{p} - \overline{q}\mathrm{q} = |\, p\,|^2 - |\, q\,|^2 = \overline{p}\mathrm{p} - \left(-\overline{q}\right)(-\mathrm{q}) = \det\left(\left[M^{-1}\right]\right)$$

$$[M]^{-1} = 1/\left(|\, p\,|^2 - |\, q\,|^2\right)\begin{bmatrix} \overline{p} & -q \\ -\overline{q} & p \end{bmatrix}$$

$$[M]^{-1}.[\mathrm{M}] = 1/\left(|\, p\,|^2 - |\, q\,|^2\right)\begin{bmatrix} \overline{p} & -q \\ -\overline{q} & p \end{bmatrix}.\begin{bmatrix} p & q \\ \overline{q} & \overline{p} \end{bmatrix}$$

$$= 1/\left(|\, p\,|^2 - |\, q\,|^2\right)\begin{bmatrix} |\, p\,|^2 - |\, q\,|^2 & \overline{p}\,q - \overline{p}\,q \\ -p\,\overline{q} + p\,\overline{q} & |\, p\,|^2 - |\, q\,|^2 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = [\mathcal{E}]$$

Given the definition of $[M]^{-1}$, we can see by inspection that it belongs to the set of matrices with conjugate pairs on the diagonals, i.e. $\begin{bmatrix} a & b \\ \overline{b} & \overline{a} \end{bmatrix}$. Respecting $[M]^{-1}$, the stipulation that |p| > |q| is guaranteed by $|\overline{p}|$ > |-q|. These structures are unaffected by the multiplier $1/\left(|\, p\,|^2 - |\, q\,|^2\right)$.

The Composition

To show that compositions with matrices like [M] preserve structure, show that diagonal opposites of [M].[N] are complex conjugates, where [N] is a matrix in the set [M]. This proof follows Vasco's answer on the VCA Forum, but some different notation is used to avoid subscripts.

Let N = $\begin{bmatrix} r & s \\ \overline{s} & \overline{r} \end{bmatrix}$, where |r| > |s|. [M] remains unchanged.

Calculate the composition

$$[M].[N] = \begin{bmatrix} p & q \\ \overline{q} & \overline{p} \end{bmatrix}.\begin{bmatrix} r & s \\ \overline{s} & \overline{r} \end{bmatrix}$$

$$= \begin{bmatrix} pr + q\,\overline{s} & ps + q\,\overline{r} \\ \overline{q}\,r + \overline{p\,s} & \overline{q}\,s + \overline{p\,r} \end{bmatrix}$$

Check that the diagonal opposites are conjugates:

$$\overline{q}\,s + \overline{p\,r} = \overline{pr\ +\ q\,\overline{s}}$$

$$\overline{q}\,r + \overline{p\,s} = \overline{ps\ +\ q\,\overline{r}}$$

One can see by inspection that diagonal opposites are conjugates. Now determine whether |p| > |q| is satisfied by $|pr + q\,\overline{s}|$ and $|\,ps + q\,\overline{r}|$.

Let P = pr + $q\,\overline{s}$ and Q = ps + $q\,\overline{r}$. Then we wish to show that |P| > |Q|.

$$|\ P\ |^2 = (p\ r + q\ \overline{s})\ (\overline{p}\,\overline{r} + \overline{q}\ s) = |p|\ |r| + p\ \overline{q}\ r\ s + \overline{p}\ q\ \overline{r}\,\overline{s} + |q|\ |s|$$

$$|\ Q\ |^2 = (p\,s + q\,\overline{r})\ (\overline{p}\,\overline{s} + \overline{q}\ r) = |p|\ |s| + p\ \overline{q}\ r\ s + \overline{p}\ q\ \overline{r}\,\overline{s} + |q|\ |r|$$

$$|\ P\ |^2 - |\ Q\ |^2 = |p|\ |r| + |q|\ |s| - |p|\ |s| - |q|\ |r|$$

$$= |p|\ (|r| - |s|) + |q|\ (|s| - |r|) = |p|\ (|r| - |s|) - |q|\ (|r| - |s|)$$

$$= (|p| - |q|)\ (|r| - |s|)$$

Since |p| > |q| and |r| > |s|, $|\ P\ |^2 - |\ Q\ |^2 > 0$, which implies that |P| > |Q|, which is what we wanted.

The given M has two obvious properties: (1) diagonal opposites are conjugate pairs; (2) |p| > |q|. We have shown that the corresponding set of Möbius matrices with these properties has three more properties necessary for the definition of a group: (3) The set includes the identity matrix [$\mathcal{E}$]; (4) every [M] in the set has an inverse $[M]^{-1}$; and (5) every composition [M].[N] of members of the set preserves the first two properties. Therefore, the set of matrices of Möbius transformations with diagonal opposite conjugates where |p| > |q| constitutes a group. Since the two by two complex matrices produce the same transformations as their corresponding Möbius transformations (P. 157, 4th •), we have also shown that the set M, where d = $\overline{a}$, c = $\overline{b}$, and |a| > |b|, forms a group.

(iii) Use the disc automorphism interpretation of these transformations to give a geometric explanation of the fact that they form a group.

From pp. 178-9, we find that

(a) $e^{i\phi}(z-a)/(\overline{a}z-1)$ is the most general Möbius automorphism of the unit disc D

(b) $M_a(z) = (z-a)/(\overline{a}z-1)$ is the most interesting part of M_a^{ϕ}

(c) $M_a = \mathcal{R}_L \circ \mathcal{I}_J$

where $\mathcal{R}_L$ is a reflection in L and $\mathcal{I}_J$ is inversion (reflection) in a circle J.

The defining quality of the set in this case is the disc automorphism. M_a maps points on the unit disc to points on the unit disc.

M has an identity element that belongs to the set. On p. 179, Needham has M_a *is involutory;* $(M_a \circ M_a) = \varepsilon$. One can demonstrate this with an expansion of $M \circ M$

$$M \circ M = (\mathcal{R}_L \circ \mathcal{I}_J) \circ (\mathcal{I}_J \circ \mathcal{R}_L)$$

$$= \mathcal{R}_L \circ \varepsilon \circ \mathcal{R}_L = \mathcal{R}_L \circ \mathcal{R}_L$$

$$= \varepsilon$$

Every M has an inverse that belongs to the set. On p. 125, we find M_a is involutory, so $M_a^{-1} = M_a$, $M_a \circ M_a = \varepsilon$, and $M_a \circ M_a(\text{p}) = \text{p}$.

The composition of two members of the set yields a third member of the set. If M_A and M_B are both Möbius automorphisms of the unit disc, then their composition is necessarily an automorphism of the unit disc.

Looking at this in terms of reflections, one could say that M_a, composed of $\mathcal{R}_L \circ \mathcal{I}_J$, maps p (a complex number on the unit disc) to $\tilde{p}$, another complex number on the unit disc. Then because M_b is also a matrix that maps a point on the disc to another point on the disc, it maps $\tilde{p}$ to a third complex number, say w, on the unit disc. Hence, $M_a \circ M_b$ meets the criterion by means of $(\mathcal{R}_L \circ \mathcal{I}_J) \circ (\mathcal{R}_L \circ \mathcal{I}_J)$. Similarly, $M_a \circ M_a(p)$ maps p to itself.

A second approach to the composition proof converting the disc automorphism definition to matrix format. The proof appears to fail in matrix composition if one must preserve the structure implied by conjugates and signs on the diagonals.

Given in Möbius format converted to matrix: $[M_a] = \begin{bmatrix} 1 & -a \\ \overline{a} & -1 \end{bmatrix}$

$$[M_a] \circ [M_b] = \begin{bmatrix} 1 & -a \\ \overline{a} & -1 \end{bmatrix} . \begin{bmatrix} 1 & -b \\ \overline{b} & -1 \end{bmatrix} = \begin{bmatrix} 1 - a\,\overline{b} & a - b \\ \overline{a} - \overline{b} & 1 - \overline{a}\,b \end{bmatrix}.$$

This has the structure $\begin{bmatrix} 1 - a\,\overline{b} & a - b \\ \overline{a - b} & \overline{1 - a\,\overline{b}} \end{bmatrix}$, which is not the same structure on the diagonals as the structure of $[M_a]$. For example 1 and –1 in $[M_a]$ are not parallel to $(1 - a\,\overline{b})$ and $(1 - \overline{a}\,b)$ in $[M_a] \circ [M_b]$, which one could regard as conjugate pairs with no change in sign. On the other diagonal, –a and $\overline{a}$ are not parallel to (a-b) and $(\overline{a} - \overline{b})$.

But perhaps the defining criterion of M_a should be whether it maps points on the disc to points on the disc. If the composite matrix is $[M_{\text{ab}}]$, then $[M_{\text{ab}}].p$ should be a complex point on the unit disc, where

$$\text{p} = p_1 + \text{i}\, p_2 \equiv \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

is a complex point on the unit disc. By inspection one can see that all four of the elements of $[M_a] \circ [M_b]$ have absolute value < 1. We also know that |p| < 1. Then $|p_1| < 1$ and $|p_2| < 1$. Then if

$$[M_a] \circ [M_b] . \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} = \begin{bmatrix} (a - b)\, p_2 \ + \ p_1 \left(1 - a\,\tilde{b}\right) \\ p_2 (1 - b\,\overline{a}) \ + \ p_1 \left(\overline{a} \ - \ \overline{b}\right) \end{bmatrix} = \begin{bmatrix} \tilde{p}_1 \\ \tilde{p}_2 \end{bmatrix} = \tilde{p}$$

it follows that on the top row |(a-b) p_2| < 1 and $\left| \ p_1 \left(1 - a\,\tilde{b}\right) \right| < 1$, and on the bottom row $\left| \ p_2 (1 - b\,\overline{a}) \right| < 1$ and $\left| \ p_1 \left(\overline{a} \ - \ \overline{b}\right) \right| < 1$, but does that entail that the sums $\tilde{p}_1$ and $\tilde{p}_2$ are also < 1? I believe it does. The matrix multiplication of $[M_a] \circ [M_b] . \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ essentially produces two inner products with real numbers, one for each row of the matrix. Because the inner product projects a row vector from $[M_a] \circ [M_b]$ onto $\begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$, and both vectors have length < 1, the projection must have length < 1. Hence, $|\tilde{p}| < 1$. Then we know that the composition of two matrices of type $[M_a]$, which is a matrix that maps the unit disc to itself, is another matrix that maps the disc to itself.