Solutions to Math 3E03 Homework 3

2.40. Let a denotes the order of y^t. By the question, we have $1 = y^m = (y^t)^d$. It follows from Lemma 2.53 (or Proposition 2.54) that $a|d$. On the other hand, we also have $1 = (y^t)^a = y^{at}$. This, again using Lemma 2.53 (or Proposition 2.54), implies that $dt|at$. In other words, $d|a$. Combining this with the above, one has $a = d$, as required.

2.42. $A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$; $A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$;

$B^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$; $B^4 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$; $B^6 = B^2B^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$.

$AB = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$

We shall show by induction that $(AB)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$ for $n > 0$. We have seen this for $n = 1$. Now suppose the equality holds for $n \geq 1$, then

$$(AB)^{n+1} = (AB)^n(AB) = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -(n+1) \\ 0 & 1 \end{pmatrix}.$$

In particular, one sees that $(AB)^n \neq I$ for $n > 0$. Hence this gives an example of A and B having finite order but AB having infinite order.

2.48. Let $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ and $\begin{pmatrix} w & y \\ x & z \end{pmatrix}$ be two matrices in $\Sigma(2, \mathbb{R})$. One computes the product of two matrices.

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} w & y \\ x & z \end{pmatrix} = \begin{pmatrix} aw + cx & ay + cz \\ bw + dx & by + dz \end{pmatrix}$$

Then one has $aw+cx+bw+dx = (a+b)w+(c+d)x = w+x = 1$ and $ay+cz+by+dz = (a+b)y + (c+d)z = y + z = 1$. Thus the matrix on the right is in $\Sigma(2, \mathbb{R})$.

Similarly, one has the inverse.

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \frac{1}{ad-bc}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

Then one has

$$\frac{d-b}{ad-bc} = \frac{d-b}{ad-b(1-d)} = \frac{d-b}{(a+b)d-b} = \frac{d-b}{d-b} = 1 \text{ and}$$

$$\frac{a-c}{ad-bc} = \frac{a-c}{a(1-c)-bc} = \frac{a-c}{a-(a+b)c} = \frac{a-c}{a-c} = 1.$$

Thus an inverse of a stochastic matrix is stochastic.

2.51. Using the property of φ being an isometry, we have the following equations

$$a^2+b^2 = |\varphi(e_1)|^2 = |(1,0)|^2 = 1;$$
$$c^2+d^2 = |\varphi(e_2)|^2 = |(0,1)|^2 = 1;$$
$$(a-c)^2+(b-d)^2 = |\varphi(e_1)-\varphi(e_2)|^2 = |(1,-1)|^2 = 2.$$

Rewriting the third equation, we have

$$a^2+b^2-2ac+b^2+d^2-2bd = 2$$

Substituting the first two equations in and upon simplifying, one has $ac+bd=0$. Now one computes

$$\begin{aligned}\det(A)^2 &= (ad-bc)^2 \\ &= a^2d^2+b^2c^2-abcd-abcd \\ &= a^2d^2+b^2c^2+a^2c^2+b^2d^2 \text{ (replace } bd \text{ by } -ac \text{ and vice versa)} \\ &= a^2(c^2+d^2)+b^2(c^2+d^2) \\ &= a^2+b^2 \\ &= 1.\end{aligned}$$

Hence $\det(A) = \pm 1$.

2.53. (i) For each $g \in G$, $g = g1 \in gH$. Since $a_1H, ..., a_tH$ are all the distinct cosets of G, necessarily $gH = a_iH$ for some i. In particular, we have $G \subseteq a_1H \cup \cdots \cup a_tH$. On the other hand, the reverse inclusion is obvious and hence the equality follows.

(ii) Let $g \in aH \cap bH$ (such a g exists since $aH \cap bH \neq \emptyset$). Then $g = ah_1 = bh_2$ for some $h_1, h_2 \in H$. (Note: h_1 and h_2 are NOT necessarily equal!)

Let $x \in aH$. Then $x = ah$ for some $h \in H$. Hence $x = ah = (ah_1)h_1^{-1}h = (bh_2)h_1^{-1}h = b(h_2h_1^{-1}h)$. Since H is a subgroup, $h_2h_1^{-1}h \in H$ and so $x \in bH$. Thus we have shown that $aH \subseteq bH$. By a similar argument, one has $bH \subseteq aH$ and so $aH = bH$.

Now if $i \neq j$, then $a_iH \neq a_jH$ and so by what we have shown above, $a_iH \cap a_jH = \emptyset$.

2.54. (i) Suppose A and B are two matrices in SL(2,$\mathbb{R}$), then one has $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$. Also $\det(A^{-1}) = (\det(A))^{-1} = (1)^{-1} = 1$. Thus SL(2,$\mathbb{R}$) is a subgroup of GL(2,$\mathbb{R}$).

(ii) Let a, b, c, d, w, x, y, z be any rational numbers. Then we have

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} w & y \\ x & z \end{pmatrix} = \begin{pmatrix} aw + cx & ay + cz \\ bw + dx & by + dz \end{pmatrix} \text{ and}$$

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \frac{1}{ad - bc} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}.$$

Since rational numbers are closed under addition and multiplication, it follows that both matrices on the right are matrices with entries in $\mathbb{Q}$.

2.57. Lagrange's Theorem tells us that $|H \cap K|$ divides $|H|$ and $|K|$. Since $\gcd(|H|, |K|) = 1$, we have $|H \cap K|$ dividing 1. Hence $H \cap K = \{1\}$.

2.60. (i) This follows from what we have done in 2.48. (Note: There seems to be a misprint here. The stochastic matrix should have columns sums being 1 as in 2.48 and not row sums equal 1 as stated here).

(ii) Every nonsingular doubly stochastic matrices has the form $\begin{pmatrix} a & 1-a \\ 1-a & a \end{pmatrix}$ for some $a \in \mathbb{R}$.

Then we have

$$\begin{pmatrix} a & 1-a \\ 1-a & a \end{pmatrix} \begin{pmatrix} b & 1-b \\ 1-b & b \end{pmatrix} = \begin{pmatrix} 2ab + 1 - a - b & a + b - 2ab \\ a + b - 2ab & 2ab + 1 - a - b \end{pmatrix} \text{ and}$$

$$\begin{pmatrix} a & 1-a \\ 1-a & a \end{pmatrix} = \frac{1}{2a-1}\begin{pmatrix} a & a-1 \\ a-1 & a \end{pmatrix}.$$

Since $(2ab+1-a-b)+(a+b-2ab)=1$ and $\frac{a+1-a}{2a-1}=1$, it follows that nonsingular stochastic matrices are closed under multiplication and inverses. Hence $\Sigma'(2,\mathbb{R})$ is a subgroup of $GL(2,\mathbb{R})$.

2.46. Let S be the set of elements of G with order not 1 or 2. For each $g \in S$, $g^{-1} \in S$ since g and g^{-1} has the same order. Also we cannot have $g = g^{-1}$ as this will imply $g^2 = 1$ contradicting our definition of S. Thus elements of order not 1 or 2 come in pairs and so $|S|$ is even. Hence the number of elements of order 2 is $|G| - |S| - 1$. (1 is to account the identity element which is the only element of order 1.) Since $|G|$ is even, this number is odd.

In particular, this number is not zero since zero is an even number. Therefore, G contains an element of order 2.

2.63. (i) Let $\alpha = (13)$. Then $\alpha\langle(12)\rangle = \{(13),(123)\}$ and $\langle(12)\rangle\alpha = \{(13),(132)\}$.

(ii) *Approach 1*: Let $a_1H, ..., a_tH$ be a list of all distinct left cosets of G and $Hb_1, ..., Hb_s$ be a list of all distinct right cosets of G. Then by question 2.53 (and its analogous for right cosets), we have

$$a_1H \cup \cdots \cup a_tH = G = Hb_1 \cup \cdots \cup Hb_s.$$

Since $|a_iH| = |H| = |Hb_j|$ and the cosets are disjoint, we have $t|H| = s|H|$ implying $t = s$. Thus the number of left cosets is equal to the number of right cosets.

Approach 2: Let S (and T) denote the set of distinct left cosets (and right cosets respectively) of H in G. Define functions $f : S \to T$ by $f(aH) = Ha^{-1}$ and $g : T \to S$ by $g(Ha) = a^{-1}H$. Now $aH = bH \iff b^{-1}a \in H \iff a^{-1}b \in H \iff Ha^{-1} = Hb^{-1}$. Thus f and g are well defined. One can check easily that f and g are mutually inverse to each other. Hence we have a bijection between S and T. In particular, they have the same number of elements.