R.K.

GROUP OF COLLEGE

Behind Kalwar Police Station, Kalwar, Jaipur (Raj.)

ASSIGNMENT

Case 1: Suppose the canonical factorisation contains one r-cycle with $r \geq 4$. Since a_i commute, we may assume that this is the first cycle $a_1 = (i_1, i_2, i_3, \ldots, i_r)$. Since N is normal, we have for $b = (i_1, i_2, i_3) \in A_n$ that the following element is in N:

$$\begin{aligned} N \ni a(ba^{-1}b^{-1}) &= (aba^{-1})b^{-1} \\ &= (a_1 b a_1^{-1})b^{-1} \\ &= [(i_1, i_2, i_3, \ldots, i_r)(i_1, i_2, i_3)(i_1, i_2, i_3, \ldots, i_r)^{-1}](i_3, i_2, i_1) \\ &= (i_2, i_3, i_4)(i_3, i_2, i_1) \quad \text{(Theorem 14.9 (7))} \\ &= (i_4, i_2, i_3)(i_3, i_2, i_1) \\ &= (i_4, i_2, i_1). \end{aligned} \tag{14.30}$$

This yields the desired 3-cycle.

Case 2: Suppose the canonical factorisation of a contains only transpositions and exactly one 3-cycle, i.e., $a = (i_1, i_2, i_3)(i_4, i_5)a_3 \cdots a_r$. For $b = (i_1, i_2, i_4) \in A_n$

$$\begin{aligned} N \ni a(ba^{-1}b^{-1}) &= \left[[(i_1, i_2, i_3)(i_4, i_5)](i_1, i_2, i_4)[(i_1, i_2, i_3)(i_4, i_5)]^{-1}\right](i_4, i_2, i_1) \\ &= (i_2, i_3, i_5)(i_4, i_2, i_1) \\ &= (i_3, i_5, i_2)(i_2, i_1, i_4) \\ &= (i_3, i_5, i_2, i_1, i_4) \end{aligned} \tag{14.31}$$

which is a 5-cycle, so we have reduced the problem to Case 1.

Case 3. Suppose the canonical factorisation of a contains more than one 3-cycle, i.e., $a = (i_1, i_2, i_3)(i_4, i_5, i_6)a_3 \cdots a_r$. For $b = (i_1, i_2, i_4) \in A_n$

$$\begin{aligned} N \ni a(ba^{-1}b^{-1}) &= \left[[(i_1, i_2, i_3)(i_4, i_5, i_6)](i_1, i_2, i_4)[(i_1, i_2, i_3)(i_4, i_5, i_6)]^{-1}\right](i_4, i_2, i_1) \\ &= (i_2, i_3, i_5)(i_4, i_2, i_1) \end{aligned} \tag{14.32}$$

and we conclude as in Case 2.

Case 4: Suppose the canonical factorisation of a contains only transpositions, $a = (i_1, i_2)(i_3, i_4)a_3 \cdots a_r$. Choose $i_5 \neq i_1, i_2, i_3, i_4$, and let $b = (i_1, i_3, i_5)$.

$$\begin{aligned} N \ni a(ba^{-1}b^{-1}) &= [a(i_1, i_3, i_5)a^{-1}](i_5, i_3, i_1) \\ &= (i_2, i_4, a(i_5))(i_5, i_3, i_1). \end{aligned} \tag{14.33}$$

If $a(i_5) = i_5$ then we obtain a 5-cycle and hence Case 1, if $a(i_5) \neq i_5$ it follows $(i_2, i_4, a(i_5)) = (a(i_1), a(i_3), a(i_5))$ and (i_5, i_3, i_1) are disjoint (since a is bijective), which yields Case 3. □

14.31. **Exercise.** Write

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 2 & 4 & 6 & 8 & 10 & 12 & 14 & 1 & 3 & 5 & 7 & 9 & 11 & 13 \end{pmatrix} \tag{14.34}$$

(1) as a product of disjoint cycles,

(2) as a product of transpositions.

Exercise 10.12.

(1) This can be either checked by a direct computation (recommended), or by the observation that the action can be represented as $(M, \xi) \mapsto M\xi$, where $M\xi$ is the standard matrix product of a 2×2 with a 2×1 matrix. Axiom (1) for group actions follows then from the associativity of matrix multiplication, and axiom (2) from $E\xi = \xi$, where E is the identity matrix.

(2) We have $G \cdot 0 = \{0\}$, so the origin $0 \in \mathbb{R}^2$ is a fixed point and orbit of the G action. Furthermore, given a point $\begin{pmatrix} x \\ y \end{pmatrix} \neq 0$, there is a matrix $M \in G$ such that $\begin{pmatrix} x \\ y \end{pmatrix} = M \begin{pmatrix} 1 \\ 0 \end{pmatrix}$; this matrix is given by $M = \begin{pmatrix} x & 0 \\ y & 1 \end{pmatrix}$ if $x \neq 0$ and $M = \begin{pmatrix} x & 1 \\ y & 0 \end{pmatrix}$ if $y \neq 0$. Hence $\mathbb{R}^2 \setminus \{0\} = G \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is the only other orbit of the G action, and 0 is the only fixed point.

Exercise 10.13.

(1) The orbits are $H \cdot \begin{pmatrix} r \\ 0 \end{pmatrix} = \left\{ \begin{pmatrix} r\cos\phi \\ r\sin\phi \end{pmatrix} : \phi \in [0, 2\pi) \right\}$ for $r \geq 0$, i.e., the origin $\{0\}$ ($r = 0$) and all circles of radius $r > 0$ centered at the origin. 0 is thus the only fixed point.

(2) The orbits are $H \cdot 0 = \{0\}$, and the rays $H \cdot \begin{pmatrix} \cos\phi \\ \sin\phi \end{pmatrix} = \left\{ \begin{pmatrix} a\cos\phi \\ a\sin\phi \end{pmatrix} : a \in \mathbb{R}_{>0} \right\}$ for $\phi \in [0, 2\pi)$. 0 is therefore again the only fixed point.

(3) The orbits are $H \cdot 0 = \{0\}$, $H \cdot \begin{pmatrix} r \\ r \end{pmatrix} = \left\{ \begin{pmatrix} ra \\ ra^{-1} \end{pmatrix} : a \in \mathbb{R}_{>0} \right\}$ for $r \in \mathbb{R} \setminus \{0\}$ (i.e., the branches of hyperbolas satisfying the equation $xy = r^2$, where r values with the same modulus but opposite sign correspond to different orbits) and $H \cdot \begin{pmatrix} r \\ -r \end{pmatrix} = \left\{ \begin{pmatrix} ra \\ -ra^{-1} \end{pmatrix} : a \in \mathbb{R}_{>0} \right\}$ for $r \in \mathbb{R} \setminus \{0\}$ (the branches of hyperbolas satisfying the equation $xy = -r^2$). 0 is the only fixed point.

(4) The orbits are the one-element sets $H \cdot \begin{pmatrix} r \\ 0 \end{pmatrix} = \left\{ \begin{pmatrix} r \\ 0 \end{pmatrix} \right\}$ for $r \in \mathbb{R}$, and the straight lines $H \cdot \begin{pmatrix} 0 \\ r \end{pmatrix} = \left\{ \begin{pmatrix} x \\ r \end{pmatrix} : x \in \mathbb{R} \right\}$ for $r \in \mathbb{R} \setminus \{0\}$. Hence $\mathrm{Fix}_H(\mathbb{R}^2) = \left\{ \begin{pmatrix} r \\ 0 \end{pmatrix} : r \in \mathbb{R} \right\}$.

(5) We have $H = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$. The H action yields $\pi/2$ rotations in $\mathbb{R}^2$ about the origin. The orbits are $H \cdot 0 = \{0\}$, $H \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \left\{ \pm \begin{pmatrix} x \\ y \end{pmatrix}, \pm \begin{pmatrix} y \\ -x \end{pmatrix} \right\}$, which are disjoint for $x > 0, y \geq 0$, say. 0 is the only fixed point.

Exercise 10.22.

(2) $(\mathbb{Z}_n, +)$ is generated by 1 and thus cyclic.

5.3. **Theorem.** Every subgroup of a cyclic group is cyclic.

Proof. Let $G = \langle g \rangle$ and $H < G$. Every $h \in H$ can be expressed as $h = g^m$ for some $m \in \mathbb{Z}$. Since the trivial group $H = \{e\}$ is cyclic we may exclude this case from now on and assume $h \neq e$. Thus there exists an element $g^m \in H$ with $m \neq 0$. Since inverse axiom $g^m \in H$ implies $g^{-m} \in H$ there is $g^m \in H$ with $m > 0$, and hence the set $I = \{k \in \mathbb{N} : g^k \in H\}$ is non-empty. Let s be the smallest element of I and g^m an arbitrary element of H. Let $q, r \in \mathbb{Z}$ be such that $m = qs + r$, $0 \leq r < s$. Now $g^r = g^{m-qs} = g^m(g^s)^{-q} \in H$. If $r \neq 0$ then $r \in I$ and we have a contradiction with s being minimal. If $r = 0$, then $m = qs$, so $g^m = (g^s)^q$, that is, $H \subseteq \langle g^s \rangle$. Since $g^s \in H$ we also have $\langle g^s \rangle \subseteq H$ and thus $H = \langle g^s \rangle$. □

Since $\mathbb{Z}$ is cyclic, we have the following classification of subgroups of $\mathbb{Z}$.

5.4. **Corollary.** Every subgroup of $\mathbb{Z}$ is of the form $s\mathbb{Z} := \{sm : m \in \mathbb{Z}\}$ with $s \in \mathbb{Z}_{\geq 0}$.

This follows directly from the previous proof: recall that 1 is the generator of $\mathbb{Z}$, and our explicit construction of the cyclic subgroups H shows that $H = s\mathbb{Z}$ in the present case.

Note that if $s > 0$ then s is the smallest integer > 0 in the subgroup.

5.5. **Definition.** Let G be a group. The **order** of $a \in G$ is the order of the cyclic group $\langle a \rangle$ and is denoted by $\operatorname{ord} a := |\langle a \rangle|$.

5.6. **Theorem.** The order of $a \in G$ is either infinite or equal to the smallest integer $s > 0$ such that $a^s = e$. In the latter case $\langle a \rangle = \{e, a, a^2, \ldots, a^{s-1}\}$.

Proof. If $a^i \neq a^j$ for all $i \neq j$, then $\operatorname{ord} a = \infty$. Otherwise there are $i < j$ such that $a^i = a^j$, and hence $a^k = e$ with $k = j - i > 0$. Let $s > 0$ be the smallest integer such that $a^s = e$. Then all elements in the set $H = \{e, a, a^2, \ldots, a^{s-1}\}$ are distinct (otherwise there would be a smaller element $k < s$ such that $a^k = e$) and is closed under multiplication since $a^s = e$. Since H is finite, this implies H is a group and thus $H = \langle a \rangle$. □

5.7. **Corollary.** Suppose $\operatorname{ord} a = s$. Then $a^k = e$ if and only if $k \in s\mathbb{Z}$.

Proof. If $k = sm$ for some $m \in \mathbb{Z}$ then $a^k = (a^s)^m = e$. On the other hand, if $a^k = e$ then $H = \{k \in \mathbb{Z} : a^k = e\}$ is a subgroup of $\mathbb{Z}$ and hence $H = s'\mathbb{Z}$ for some integer $s' > 0$ (Corollary 5.4). By Theorem 5.6 s is the smallest integer > 0 such that $a^s = e$ and so $s = s'$. □

5.8. **Theorem.** Suppose $\operatorname{ord} a = n$. Then for all $m \in \mathbb{Z}$

$$\operatorname{ord} a^m = \frac{n}{\gcd(m, n)}. \tag{5.1}$$

Proof. Let $d = \gcd(m, n)$, $m = dm'$, $n = dn'$, with m', n' coprime. Set $r = \operatorname{ord} a^m$. Since $e = (a^m)^r = a^{mr}$ we have by Corollary 5.7 $mr = nt$ for some $t \in \mathbb{Z}$. Divide by d to obtain $m'r = n't$. Since m', n' are coprime n' divides r, so $n' \leq r$. On the other hand $(a^m)^{n'} = (a^n)^{m'} = e^{m'} = e$ so $r \leq n'$. We conclude $r = n'$. □

The following two corollaries follow directly from the above theorem.

5.9. **Corollary.** If $\operatorname{ord} a = n$ then $\langle a \rangle = \langle a^m \rangle$ if and only if m, n are coprime.

3.1. **Definition.** A non-empty subset $H \subseteq G$ is called a **subgroup**, if H is a group with respect to the same composition as in G; we will write in this case $H \leq G$.

H is called a **proper subgroup** if $H \neq G$; we write $H < G$.

3.2. **Example.**

(1) $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$.
(2) If $d \in \mathbb{N}$ divides $n \in \mathbb{N}$, then $(n\mathbb{Z}, +) \leq (d\mathbb{Z}, +)$.
(3) The groups in Example 1.8 and Exercise 2.3 are subgroups of $GL(2, \mathbb{R})$.

3.3. **Theorem.** Let G be a group and $H \subseteq G$ a non-empty subset. Then H is a subgroup if and only if

$$(a, b \in H) \Rightarrow (ab \in H \text{ and } a^{-1} \in H). \tag{3.1}$$

Proof. Assume H is a subgroup. Then the image of $H \times H$ under the composition $\circ : G \times G \to G$ satisfies $\circ(H, H) \subseteq H$, i.e., $ab \in H$ for all $a, b \in H$. If e is the identity in H, we have $e^2 = e$, but this means by Lemma 1.3 that e is also the identity in G. Hence the inverse of a in H is also the inverse of a in G, and so $a^{-1} \in H$.

Conversely, assume (3.1). Then the composition $\circ$ on G, restricted to H, yields a map $H \times H \to H$, $(a, b) \mapsto ab$. The map is clearly associative (since this is true in the full set G), and we only need to show that the identity e in G is contained in H. But this follows from taking $b = a^{-1}$ in (3.1). □

3.4. **Corollary.** Let G be a group and $H \subseteq G$ a non-empty subset. Then H is a subgroup if and only if

$$(a, b \in H) \Rightarrow (ab^{-1} \in H). \tag{3.2}$$

Proof. Assume H is a subgroup. Let $a, b \in H$. Then, by Theorem 3.3, $b^{-1} \in H$ and $ab^{-1} \in H$. On the other hand, assume (3.2) holds. In particular (for $a = e$) $b \in H$ implies $b^{-1} \in H$ and hence $(a, b \in H) \Rightarrow (a, b^{-1} \in H) \Rightarrow (ab \in H)$ by (3.2). Thus by Theorem 3.3 H is a subgroup. □

3.5. **Theorem.** Let G be a group and $H \subseteq G$ a **finite** non-empty subset. Then H is a subgroup if and only if

$$(a, b \in H) \Rightarrow (ab \in H). \tag{3.3}$$

Proof. The first implication follows from the previous theorem. Hence assume (3.3) holds. Since G is a group, for every fixed $a \in G$ the map $G \to G$, $x \mapsto ax$, is injective. If $a \in H$, then the restriction of this map to H yields, in view of (3.3), a the map $H \to H$, $x \mapsto ax$, which is still injective. But since H is finite, injective implies surjective and hence bijective. Hence if $y = ax \in H$, the inverse map is $H \to H$,

$y \mapsto x = a^{-1}y$. The choice $y = a$ implies $e \in H$ and the choice $y = e$ implies $a^{-1} \in H$. □

3.6. **Example.** Let $G = \{e, a, b, c\}$ be the Klein four group as defined in 1.13. The above theorem shows that $\{e, a\}$, $\{e, b\}$, $\{e, c\}$ are subgroups of G.

3.7. **Theorem.** Consider the groups $H_1 \leq G_1$, $H_2 \leq G_2$ and let $\varphi : G_1 \to G_2$ be a homomorphism. Then

(1) the image $\varphi(H_1)$ is a subgroup of G_2.
(2) the pre-image $\varphi^{-1}(H_2)$ is a subgroup of G_1.

Proof. (1) $\varphi(H_1)$ is evidently non-empty. We have for $a, b \in H_1$ that $\varphi(a)\varphi(b) = \varphi(ab) \in \varphi(H_1)$ and $\varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(H_1)$. The claim follows from Theorem 3.3.

(2) Clearly $e \in \varphi^{-1}(H_2)$ and the latter is non-empty. $a, b \in \varphi^{-1}(H_2)$ implies $\varphi(a), \varphi(b) \in H_2$ and hence $\varphi(ab) = \varphi(a)\varphi(b) \in H_2$ and $\varphi(a)^{-1} = \varphi(a^{-1}) \in H_2$. Therefore $ab, a^{-1} \in \varphi^{-1}(H_2)$, and claim (2) follows from Theorem 3.3. □

3.8. **Corollary.** Let $\varphi : G_1 \to G_2$ be a homomorphism.

(1) $\operatorname{im} \varphi$ is a subgroup of G_2.
(2) $\ker \varphi$ is a subgroup of G_1.