

Solution to Homework # 8 (week of 10/11–10/15)

10/12/04 Radford

1. (**18 points total**) a) In light of the comments at the beginning of the description of the problem $f' \circ f$ is a set bijection. Let $a, b \in G$. To complete the proof that $f' \circ f$ is an isomorphism we use the fact that f, f' are isomorphisms to compute that

$$\begin{aligned}(f' \circ f)(ab) &= f'(f(ab)) \\ &= f'(f(a)f(b)) \\ &= f'(f(a))f'(f(b)) \\ &= ((f' \circ f)(a))((f' \circ f)(b)).\end{aligned}$$

(**3 points**)

b) In light of the comments at the beginning of the description of the problem f'^{-1} is a set bijection. Let $a', b' \in G'$. To complete the proof that f'^{-1} is an isomorphism we use the fact that f is an isomorphism to compute that

$$\begin{aligned}f^{-1}(a'b') &= f^{-1}((f(f^{-1}(a')))(f(f^{-1}(b')))) \\ &= f^{-1}(f(f^{-1}(a')f^{-1}(b'))) \\ &= (f^{-1} \circ f)(f^{-1}(a')f^{-1}(b')) \\ &= f^{-1}(a')f^{-1}(b')\end{aligned}$$

since $f' \circ f = \text{Id}$. (**3 points**)

c) $\text{Id} : G \rightarrow G$ is a set bijection which is an isomorphism since $\text{Id}(ab) = ab = \text{Id}(a)\text{Id}(b)$ for all $a, b \in G$. Thus $\text{Id} \in \text{Aut}(G)$ and is the identity element. Let $f, g \in \text{Aut}(G)$. Then $g^{-1} \in \text{Aut}(G)$ by part b). By part a) the product $f \circ g \in \text{Aut}(G)$. Function composition is associative. Thus $\text{Aut}(G)$ is a group. (**3 points**)

d) Note $\phi_e(x) = ex = x = \text{Id}(x)$ for all $x \in G$. Therefore $\phi_e = \text{Id}$. Let $a, b \in G$. The calculation

$$(\phi_a \circ \phi_b)(x) = \phi_a(\phi_b(x)) = \phi_a(bx) = a(bx) = (ab)x = \phi_{ab}(x)$$

for all $x \in G$ shows that $\phi_a \circ \phi_b = \phi_{ab}$. (**3 points**)

e) Let $a, x, y \in G$. Then (omitting the associative calculations)

$$\phi_a(xy) = axya^{-1} = axeya^{-1} = axa^{-1}aya^{-1} = \phi_a(x)\phi_a(y).$$

Thus $\phi_a(xy) = \phi_a(x)\phi_a(y)$. Now

$$\phi_a \circ \phi_{a^{-1}} = \phi_{aa^{-1}} = \phi_e = \text{Id}$$

and

$$\phi_{a^{-1}} \circ \phi_a = \phi_{a^{-1}a} = \phi_e = \text{Id}$$

by part d). Therefore ϕ_a has an inverse which is $(\phi_a)^{-1} = \phi_{a^{-1}}$. Thus $\phi_a : G \rightarrow G$ is an isomorphism. (**3 points**)

f) Suppose that $f \in \text{Aut}(G)$ and $a \in G$. Since f is an isomorphism

$$(f \circ \phi_a)(x) = f(\phi_a(x)) = f(ax) = f(a)f(x) = \phi_{f(a)}(f(x)) = (\phi_{f(a)} \circ f)(x)$$

for all $x \in G$. Therefore $f \circ \phi_a = \phi_{f(a)} \circ f$. (**3 points**)

2. (**13 points total**) a) Since $(1\ 2)^2 = \text{Id}$ it follows that $H = \{\text{Id}, (1\ 2)\}$.

$$\text{Id}H = H = \{\text{Id}, (1\ 2)\}$$

$$(1\ 3)H = \{(1\ 3)\text{Id}, (1\ 3)(1\ 2)\} = \{(1\ 3), (1\ 2\ 3)\}$$

$$(2\ 3)H = \{(2\ 3)\text{Id}, (2\ 3)(1\ 2)\} = \{(2\ 3), (1\ 3\ 2)\}.$$

Since every element of G is contained in one of these left cosets, the left cosets listed must be all of the left cosets of H in G . (**3 points**)

b)

$$H\text{Id} = H = \{\text{Id}, (1\ 2)\}$$

$$H(1\ 3) = \{\text{Id}(1\ 3), (1\ 2)(1\ 3)\} = \{(1\ 3), (1\ 3\ 1)\}$$

$$H(2\ 3) = \{\text{Id}(2\ 3), (1\ 2)(2\ 3)\} = \{(2\ 3), (1\ 2\ 3)\}.$$

Since every element of G is contained in one of these right cosets, the right cosets listed must be all of the right cosets of H in G . *Observe that the left cosets of H in G are not the right cosets of H in G .* (**3 points**)

c) Since $(1\ 2\ 3)^3 = \text{Id}$ and $(1\ 2\ 3)^2 = (1\ 3\ 2)$ it follows that $H = \{\text{Id}, (1\ 2\ 3)\}$.

$$\text{Id}K = K = \{\text{Id}, (1\ 2\ 3), (1\ 3\ 2)\}$$

$$(1\ 3)K = \{(1\ 3)\text{Id}, (1\ 3)(1\ 2\ 3), (1\ 3)(1\ 3\ 2)\} = \{(1\ 3), (1\ 2), (2\ 3)\}.$$

Since every element of G is contained in one of these left cosets, the left cosets listed must be all of the left cosets of K in G .

$$K\text{Id} = K = \{\text{Id}, (1\ 2\ 3), (1\ 3\ 2)\}$$

$$K(1\ 3) = \{\text{Id}(1\ 3), (1\ 2\ 3)(1\ 3), (1\ 3\ 2)(1\ 3)\} = \{(1\ 3), (2\ 3), (1\ 2)\}.$$

Since every element of G is contained in one of these cosets, the cosets listed must be all

of the right cosets of K in G . Observe that the left cosets of K in G are the right cosets of K in G . (**3 points**)

d) Let H be a subgroup of G . By Lagrange's Theorem $|H| = 1, 2, 3, 6$ as $|G| = 6$. We consider these cases in turn.

Case 1: $|H| = 1$. In this case $H = (e)$

Case 2: $|H| = 2$. By Lagrange's Theorem $|a| = |\langle a \rangle|$ is 1 or 2 or all $a \in H$. In the former case $a = e$. Therefore there is an element a in H of order 2. In this case $H = \langle a \rangle$. Conversely, if $a \in G$ has order 2 then $\langle a \rangle$ has order 2. Therefore the subgroups of order 2 are:

$$\langle (12) \rangle = \{Id, (12)\}, \quad \langle (13) \rangle = \{Id, (13)\}, \quad \langle (23) \rangle = \{Id, (23)\}.$$

Case 3: $|H| = 3$. By Lagrange's Theorem $|a| = |\langle a \rangle|$ is 1 or 3 or all $a \in H$. In the former case $a = e$. Therefore there is an element a in H of order 3. In this case $H = \langle a \rangle$. Conversely, if $a \in G$ has order 3 then $\langle a \rangle$ has order 3. Since (123) and $(123)^2 = (132)$ are the elements of G of order 3, there is one subgroup of order 3, namely:

$$\langle (123) \rangle = \{Id, (123), (132)\}.$$

Case 4: $|H| = 6$. Necessarily $H = G$. (**4 points**)

3. (**9 points total**) a) Suppose that G is *not* cyclic. Let $a \in G$. By Lagrange's Theorem $|\langle a \rangle| = 1, p$, or p^2 . Since G is not cyclic the latter is ruled out. Therefore $|\langle a \rangle| = 1$, in which case $a = e$ and consequently $a^p = e$, or $|\langle a \rangle| = p$, in which case $a^p = e$. We have shown in any event $a^p = e$. (**3 points**)

b) Let $x \in G$. By part a) the equation $x^2 = e$ holds. The equations $xe = x = ex$ and $x^2 = e$ for all $x \in G$ enable us to fill out the Cayley table in part:

	e	a	b	c	
e	e	a	b	c	
a	a	e			.
b	b		e		
c	c			e	

Since every element of G must appear once in each row and each column necessarily

	e	a	b	c	
e	e	a	b	c	
a	a	e	c	b	. (3 points)
b	b	c	e	a	
c	c	b	a	e	

c) There are several possibilities. We describe two here by giving their Cayley tables.

	Id	(1 2)	(3 4)	(1 2)(3 4)
Id	Id	(1 2)	(3 4)	(1 2)(3 4)
(1 2)	(1 2)	Id	(1 2)(3 4)	(3 4)
(3 4)	(3 4)	(1 2)(3 4)	Id	(1 2)
(1 2)(3 4)	(1 2)(3 4)	(3 4)	(1 2)	Id

and

	Id	(1 2)(3 4)	(1 3)(2 4)	(1 4)(2 3)
Id	Id	(1 2)(3 4)	(1 3)(2 4)	(1 4)(2 3)
(1 2)(3 4)	(1 2)(3 4)	Id	(1 4)(2 3)	(1 3)(2 4)
(1 3)(2 4)	(1 3)(2 4)	(1 4)(2 3)	Id	(1 2)(3 4)
(1 4)(2 3)	(1 4)(2 3)	(1 3)(2 4)	(1 2)(3 4)	Id

(3 points)