Math 516 **Fall 2008** **Radford**

Written Homework # 2 Solution

10/09/08

---

1. (**20 points**) The challenge of part (a) is not to fall asleep. A part of basic algebra is checking mundane details. Let $f, g, h \in \mathcal{G}$.

(a) (**9 pts**) Let $i \in I$. Since the binary operation in G_i is associative

$$\begin{aligned}((fg)h)(i) &= ((fg)(i))h(i) \\ &= (f(i)g(i))h(i) \\ &= f(i)(g(i)h(i)) \\ &= f(i)((gh)(i)) \\ &= (f(gh))(i).\end{aligned}$$

We have shown that $(fg)h = f(gh)$.

Let e_i be the identity element of G_i for all $i \in$ and define $e \in \mathcal{G}$ by $e(i) = e_i$ for all $i \in I$. Then

$$(fe)(i) = f(i)e(i) = f(i)e_i = f(i) = e_i f(i) = (ef)(i)$$

for all $i \in I$ means that $fe = f = ef$. Thus e is an identity element for $\mathcal{G}$.

Define $f' \in \mathcal{G}$ by $f'(i) = f(i)^{-1}$ for all $i \in I$. The calculations

$$(ff')(i) = f(i)f'(i) = f(i)f(i)^{-1} = e_i = e(i)$$

and

$$(f'f)(i) = f'(i)f(i) = f(i)^{-1}f(i) = e_i = e(i)$$

show that $ff' = e = f'f$. Therefore f has an inverse which is f'.

(b) (**11 pts**) Tables for finite groups have the property that each element of the group must appear exactly once in each row and in each column (cancellation property). We may write $G = \{e, a, b, c\}$, where e is the identity element of G.

Case 1: $x^2 = e$ for all $x \in G$. Then the table looks like

	e	a	b	c
e	e	a	b	c
a	a	e	·	·
b	b	·	e	·
c	c	·	·	e

We are forced to fill in the columns (left to right)

	e	a	b	c
e	e	a	b	c
a	a	e	·	·
b	b	**c**	e	·
c	c	**b**	·	e

	e	a	b	c
e	e	a	b	c
a	a	e	**c**	·
b	b	c	e	·
c	c	b	**a**	e

	e	a	b	c
e	e	a	b	c
a	a	e	c	**b**
b	b	c	e	**a**
c	c	b	a	e

Thus the table must be

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

$\mathbf{Z}_2 \times \mathbf{Z}_2$ realizes the table. Let $x = (1,0)$ and $y = (0,1)$. Set $z = x + y = (1,1)$ and $0 = (0,0)$. Then the table for $\mathbf{Z}_2 \times \mathbf{Z}_2$ is

	0	x	y	z
0	0	x	y	z
x	x	0	z	y
y	y	z	0	x
z	z	y	x	0

Thus $f : \mathbf{Z}_2 \times \mathbf{Z}_2 \longrightarrow G$ given by

$$f(0) = e, \quad f(x) = a, \quad f(y) = b, \quad f(z) = c$$

is an isomorphism of groups.

Case 2: $x^2 \neq e$ for some $x \in G$. We may assume $a^2 = b \neq e$ (Why?) Thus the table looks like

	e	a	b	c
e	e	a	b	c
a	a	b	·	·
b	b	·	·	·
c	c	·	·	·

The second row and second column must be filled in

	e	a	b	c
e	e	a	b	c
a	a	b	**c**	**e**
b	b	**c**	·	·
c	c	**e**	·	·

which forces

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	**e**	·
c	c	e	**a**	·

and

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	**a**
c	c	e	a	**b**

Thus the table is

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

The table for $\mathbf{Z}_4$ is given by

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Thus $f : \mathbf{Z}_4 \longrightarrow G$ given by

$$f(0) = e, \quad f(1) = a, \quad f(2) = b, \quad f(3) = c$$

is an isomorphism.

2. (**20 points**) The condition $a^2 = e$ for all $a \in G$ is equivalent to $a = a^{-1}$ for all $a \in G$.

(a) (**7 pts**) Let $a, b \in G$. From $abab = (ab)^2 = e$ we deduce $ab = b^{-1}a^{-1} = ba$.

(b) (**13 pts**) If $|G| = 1, 2$ we are done.

Note: The condition $0 \leq i < n$ should have been $0 < i \leq n$.

Suppose $|G| > 2$. Since G is abelian G is not simple; else, since all subgroups of G are normal by part (a), G is cyclic and $G \simeq \mathbf{Z}_2$ as $G = <a>$ for some $a \in G$ and $a^2 = e$. Therefore there is a (normal) subgroup H of G which satisfies $(e) \neq H \neq G$. Since G is finite there is a maximal such subgroup which we call, by slight abuse of notation, H as well.

¿From $|G| = |G/H||H|$ we now conclude that $1 < |G/H|, |H| < |G|$. By the Fourth Isomorphism Theorem G/H is simple. Thus G/H is cyclic of order 2, by our argument above, which means $|G : H| = 2$.

By induction on $|G|$ there is an $m \geq 0$ and a chain of subgroups $(e) = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_m = H$ such that $|H_i : H_{i-1}| = 2$ for all $0 < i \leq m$. Set $n = m + 1$ and $G = H_n$. Thus our conclusion follows by induction on $|G|$.

3. (**15 points**) Let $a \in G$. Then $a \in S$ for a unique $S \in \mathcal{G}$ since $\mathcal{G}$ partitions G. Therefore $\pi : G \longrightarrow \mathcal{G}$ given by $\pi(a) = S$ is a well-defined function.

Now suppose $b \in \mathcal{G}$ and let $T \in \mathcal{G}$ satisfy $b \in T$. Then $ab \in ST$ and $ST \in \mathcal{G}$ by assumption. Therefore $\pi(ab) = ST = \pi(a)\pi(b)$ which means that π is a group homomorphism.

Suppose $N \in \mathcal{G}$ satisfies $e \in N$. Then $N = \pi(e)$ is the neutral element of $\mathcal{G}$. As

$$S = \pi^{-1}(\{S\}) = \pi^{-1}(\{\pi(a)\}) = a(\ker \pi) = (\ker \pi)a$$

and $N = \pi^{-1}(\{N\}) = \ker \pi$ we conclude that $S = aN = Na$.

4. (**20 points**)

(a) (**5 pts**) $e \in H$ as $f(e) = e' = g(e)$; thus $H \neq \emptyset$. Let $a, b \in H$. The calculation

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = g(a)g(b)^{-1} = g(a)g(b^{-1}) = g(ab^{-1})$$

shows that $ab^{-1} \in H$. Therefore $H \leq G$.

(b) (**5 pts**) *Only if.* Suppose $f = g$. Then $f(a) = g(a)$ for all $a \in G$; in particular $f(s) = g(s)$ for all $s \in S$. *If*: Suppose that $f(s) = g(s)$ for all $s \in S$. Then $S \subseteq H$ and consequently $<S> \subseteq H$ since the latter is a subgroup of G. Therefore $G = <S> \subseteq H (\subseteq G)$ from which $G = H$ follows. We have shown that $f(a) = g(a)$ for all $a \in G$, or equivalently $f = g$.

(c) (**5 pts**) First of all suppose that S is any subset of G and $a \in G$ satisfies $sa = as$ for all $s \in S$. Then $S \subseteq \mathrm{C}_G(\{a\})$ which means $<S> \subseteq \mathrm{C}_G(\{a\})$ since the latter is a subgroup of G.

Now let S, T be as in part (c) and let $t \in T$. Since $st = ts$ for all $s \in S$, $H = <S> \subseteq \mathrm{C}_G(\{t\})$. We have shown $ht = th$ for all $h \in H$.

Now let $h \in H$. Then $T \subseteq \mathrm{C}_G(\{h\})$ and thus $K = <T> \subseteq \mathrm{C}_G(\{h\})$. Therefore $hk = kh$ for all $k \in K$.

(d) (**5 pts**) By part (c) $HK = KH$ and therefore $HK \leq G$. Let $a, a' \in HK$. Then $a = hk$ and $a' = h'k'$ for some $h, h' \in H$ and $k, k' \in K$. Therefore

$$aa' = hkh'k' = hh'kk' = h'hk'k = h'k'hk = a'a$$

which shows that HK is commutative.

5. (**25 points**) For $a \in G$, where G is a finite group, recall that the order of a, denoted $|a|$, is the least positive integer n satisfying $a^n = e$ and $|a| = |<a>|$.

(a) (**5 pts**) $(ab)^m = a^m b^m = eb^m$. Thus $<b^m> \subseteq <ab>$. Since $<b^m> = <b^{(m,n)}> = <b>$, by Lagrange's Theorem $m||<ab>|$. Since $ba = ab$ and $(n, m) = 1$, we conclude $n||<ab>|$. Thus $mn||<ab>|$ since $(m, n) = 1$. The calculation $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e^n e^m = e$ shows that $|<ab>||mn$. Therefore $mn = |<ab>| = |ab|$.

(b) (**5 pts**) The possible orders of elements of G are 1, 2, 3, or 6 since $|G| = 6$. We will show that $x^2 = e$ for all $x \in G$ or $x^3 = e$ for all $x \in G$ are not possible.

$x^2 = e$ for all $x \in G$ is ruled out by Problem 2 since $|G| \neq 2^n$ for all $n \geq 0$. Suppose $x^3 = e$ for all $x \in G$. Then G has different subgroups H, K of order 3. Since $H \cap K = H$ implies $H \subseteq K$ and consequently $H = K$, $H \cap K \neq K$. By Lagrange's Theorem $H \cap K = (e)$. Thus $|G| \geq |HK| = |H||K|/|H \cap K| = 9 > |G|$, a contradiction. Thus $x^3 = e$ for all $x \in G$ is ruled out.

Since $|G| \neq 2^n$ for all $n \geq 0$, by Problem 2, $a^2 \neq e$ for some $a \in G$. Thus G has an element of order 3 or 6. In the latter case $G \simeq \mathbf{Z}_6$. Thus we may assume that G has an element a of order 3.

Our conclusion: either G has an element of order 6 or elements a, b of orders 2 and 3 respectively. By part (a) the product ab has order 6. Thus G has an element of order 6 which means $G \simeq \mathbf{Z}_6$.

(c) (**5 pts**) Observe that $\mathrm{Z}(G) = (e)$ since G is non-abelian. Otherwise $\mathrm{Z}(G)$ has order 2 or 3 by Lagrange's Theorem. Since $|G| = 6$, by the same if $L \leq G$ and $\mathrm{Z}(G) \subseteq L$ then $L = \mathrm{Z}(G)$ or $L = G$. Since G is not abelian there ia a $a \not{i}n\mathrm{Z}(G)$. By Problem 4 $L = <a>\mathrm{Z}(G)$ is an abelian subgroup of G which properly contains $\mathrm{Z}(G)$. Thus $L = G$, a contradiction. W have Shown $\mathrm{Z}(G) = (e)$.

The class equation reduces to $6 = 1 + \ell 2 + m3 + n6$ for some $\ell, m, n \geq 0$. Therefore $\ell = m = 1$ and $n = 0$.

(d) (**5 pts**) More generally, suppose that G is any group and $H = <a> \trianglelefteq G$ has 2 elements. Let $g \in G$. Then $\{e, a\} = H = gHg^{-1} = \{geg^{-1}, gag^{-1}\} = \{e, gag^{-1}\}$ means $gag^{-1} = a$. Therefore $a \in \mathrm{Z}(G)$ which means $H \subseteq \mathrm{Z}(G)$.

Since $\mathrm{Z}(G) = (e)$ for our particular G, which wasshown for part (c), H is not normal.

(e) (**5 pts**) Note that $\mathrm{Ker}\,\pi \subseteq H$. Since $|H| = 2$ either $\mathrm{Ker}\,\pi = (e)$ or $\ker\pi = H$. As $\mathrm{Ker}\,\pi$ is a normal subgroup of G and, by part (d), H is not, $\mathrm{Ker}\,\pi = (e)$. Therefore π is injective and thus bijective since $|G| = 6 = |S_A|$.