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

Written Homework # 1 Solution

10/13/08

---

1. (**20 points**)

(a) (**8 pts**) This is straightforward. $a^{m+0} = a^m = a^m e = a^m a^0$; thus the formula holds when $n = 0$. Suppose $n \geq 0$ and the formula holds. Then $a^{m+(n+1)} = a^{(m+n)+1} = a^{m+n}a = (a^m a^n)a = a^m(a^n a) = a^m a^{(n+1)}$. Thus the formula holds for $n + 1$ By induction the formula holds for all $n \geq 0$.

(b) (**6 pts**) Several cases. Let $m, n \geq 0$. In light of part (a) it suffices to establish:

$$a^{m-n} = a^m a^{-n}; \tag{1}$$

$$a^{-m+n} = a^{-m} a^n; \tag{2}$$

$$a^{-m-n} = a^{-m} a^{-n}. \tag{3}$$

Since the exponents in (3) are negative, by part (a), replacing a by a^{-1},

$$a^{-m-n} = a^{-(m+n)} = (a^{-1})^{m+n} = (a^{-1})^m (a^{-1})^n = a^{-m} a^{-n}.$$

We need only establish (1) and (2).

Suppose $m - n \geq 0$. Then by part (a) $a^m = a^{(m-n)+n} = a^{m-n}a^n$. Therefore $a^m(a^n)^{-1} = a^{m-n}$. Using part (a), *by induction on* $n \geq 0$ *it follows that* $(a^n)^{-1} = a^{-n}$. Thus (1) holds when $m - n \geq 0$. Writing $a^m = a^{n+(m-n)}$, the preceding calculations show that $a^m a^{-n} = a^{-n} a^m$. Now it is easy to see that all powers of a commute. Noting that $-(n - m) \geq 0$ when $m - n < 0$, (1) is established.

Note that (2) follows from (1) at this point.

(c) (**6 pts**) (Sketch) When $m, n \geq 0$ the formula follows by induction on n. Noting that $(a^m)^{-1} = a^{-m} = (a^{-1})^m$ for $m \geq 0$ the other cases follow.

2. (**20 points**)

(a) (**5 pts**) $s^2(i) = s(s(i)) = -(-i) = i$ for all $i \in \mathbf{Z}_n$. By induction on ℓ it follows that $r^\ell(i) = i + \ell$ for all $i \in \mathbf{Z}_n$ and $0 \leq \ell < n$ (that is for $\ell \in \mathbf{Z}_n$). Therefore $r^n(i) = r(r^{n-1}(i)) = r(i + (n-1)) = i + (n-1) + 1 = i$ for all $0 \leq i < n$. Therefore $s^2 = I = r^n$. Now $(srs)(i) = s(r(s(i))) = s(r(-i)) = s(-i + 1) = -(-i + 1) = i - 1 = i + (n-1) = r^{(n-1)}(i)$ for all $i \in \mathbf{Z}_n$. Now $r^{-1} = r^{(n-1)}$ since $r^n = I$. Therefore $srs = r^{(n-1)} = r^{-1}$.

(b) (**5 pts**) Observe that $s^\ell(i) = (-1)^\ell i$ for $0 \leq \ell < 2$ and $i \in \mathbf{Z}_n$. Thus $r^k s^\ell(i) = r^k(s^\ell(i)) = r^k((-1)^\ell i) = (-1)^\ell i + k$ for all $i \in \mathbf{Z}_n$.

Now suppose that $0 \leq \ell, \ell' < 2$ and $0 \leq k, k' < n$ and $s^\ell r^k = s^{\ell'} r^{k'}$. Applying both sides of this equation to $i \in \mathbf{Z}_n$ gives

$$(-1)^\ell i + k = (-1)^{\ell'} i + k'$$

for all $i \in \mathbf{Z}_n$. Setting $i = 0$ we see that $k = k'$. Setting $i = 1$ gives $(-1)^\ell = (-1)^{\ell'} \in \mathbf{Z}_n$. Therefore ℓ, ℓ' are both even or are both odd since $-1 \neq 1$. *The latter follows since* $n > 2$. Thus $\ell = \ell'$ since $0 \leq \ell, \ell' < 2$.

We have shown that the elements listed in part (b) are distinct; thus there are $2n$ of them. Since $|D_{2n}| = 2n$ part (b) follows.

(c) (**5 pts**) Here Problem 1 comes into play also. $sr^0 s = ss = I = r^0 = r^{(n-1)0}$ and if the formula holds for $\ell \geq 0$ then $sr^{\ell+1}s = sr^\ell rs = sr^\ell ssrs = r^{(n-1)\ell} r^{(n-1)} = r^{(n-1)\ell+(n-1)} = r^{(n-1)(\ell+1)}$. Thus $sr^\ell s = r^{(n-1)\ell}$ for all $\ell \geq 0$ by induction on ℓ. As $r^{(n-1)} = r^{-1}$, $r^{(n-1)\ell} = (r^{(n-1)})^\ell = (r^{-1})^\ell = r^{-\ell}$ for $\ell \geq 0$.

(d) (**5 pts**) Let $\ell \geq 0$. Then $s^0 r^\ell s^0 = r^\ell$ and, by part (c), $s^1 r^\ell s^1 = r^{(n-1)\ell}$. Note $s = s^{-1}$. Therefore $s^i r^\ell s^i = r^{(n-1)^i \ell}$, or equivalently $s^i r^\ell = r^{(n-1)^i \ell} s^i$, for all $0 \leq i < 2$ and $\ell \geq 0$. Therefore

$$(r^\ell s^i)(r^{\ell'} s^{i'}) = r^\ell s^i r^{\ell'} s^{i'} = r^\ell r^{(n-1)^i \ell'} s^i s^{i'} = r^{\ell+(n-1)^i \ell'} s^{i+i'};$$

take $i'' = i + i'$ and $\ell'' = \ell + (n-1)^i \ell'$.

3. (**20 points**) We will assume $f(e) = e'$ and $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$.

(a) (**3 pts**) Since $A \leq G$, by definition $A \neq \emptyset$. Therefore $f(A) \neq \emptyset$.

Suppose $x, y \in f(A)$. Then $x = f(a)$ and $y = f(b)$ for some $a, b \in A$. Thus $xy^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) \in f(A)$ as $ab^{-1} \in A$. Therefore $f(A) \leq G'$.

(b) (**3 pts**) first of all $e' \in A'$ since $A' \leq G'$. Thus $e \in f^{-1}(A')$ as $f(e) = e'$. Therefore $f^{-1}(A') \neq \emptyset$.

Suppose $a, b \in f^{-1}(A')$. Then $f(a), f(b) \in A'$. Therefore $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} \in A'$ since $A' \leq G'$. Thus $ab^{-1} \in f^{-1}(A')$. We have shown $f^{-1}(A') \leq G$.

(c) (**3 pts**) We first show that $f(a^n) = f(a)^n$ for all $n \geq 0$ by induction on n. Since $f(a^0) = f(e) = e' = f(a)^0$ the statement is true for $n = 0$.

Suppose the statement is true for $n \geq 0$. Then $f(a)^{n+1} = f(a)^n f(a) = f(a^n)f(a) = f(a^n a) = f(a^{n+1})$. Thus the statement is true for all $n \geq 0$ by induction on n.

If $n < 0$ then $-n > 0$ and by the preceding calculation $f(a^n) = f((a^{-1})^{-n}) = f(a^{-1})^{-n} = (f((a)^{-1})^{-n}) = f(a^n)$.

(d) (**3 pts**) We establish the contrapositive. Suppose that $|a| = n < \infty$. Then $e' = f(e) = f(a^n) = f(a)^n$ shows that $|f(a)| < \infty$.

(e) (**3 pts**) We continue with part (d). $f(a)^n = e'$ means that $f(a)$ has finite order m and $m|n$ by Theorem 1(b) of "Supplement to Section 2.3".

(f) (**3 pts**) By part (e) $|f(a)|$ is finite and $|f(a)| \leq |a|$. Replacing f by f^{-1} we conclude $|a| = |f^{-1}(f(a))|$ is finite and $|a| \leq |f(a)|$. Therefore $|a| = |f(a)|$.

(g) (**2 pts**) If $n = 1$ then both $\mathbf{Z}_{n^2}$ and $\mathbf{Z}_n$, hence $\mathbf{Z}_n \times \mathbf{Z}_n$, are the trivial group with one element. Thus $\mathbf{Z}_{n^2} \simeq \mathbf{Z}_n \times \mathbf{Z}_n$ when $n = 1$.

Suppose $\mathbf{Z}_{n^2} \simeq \mathbf{Z}_n \times \mathbf{Z}_n$. Since $\mathbf{Z}_{n^2}$ has an element of order n^2, and the orders of elements of $\mathbf{Z}_n$, hence $\mathbf{Z}_n \times \mathbf{Z}_n$, divide n, it follows that $n^2 | n$. Therefore $n|1$ or equivalently $n = 1$.

4. (**20 points**) Let $g, g' \in G$. Then $g = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$, $g' = \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix}$ for some $a, a', b, b', c, c' \in$ $\mathbf{R}$. Observe that $gg' = \begin{pmatrix} 1 & a'+a & b'+ac'+b \\ 0 & 1 & c'+c \\ 0 & 0 & 1 \end{pmatrix}$, and therefore $g'g = \begin{pmatrix} 1 & a+a' & b+a'c+b' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix}$.

(a) (**5 pts**) No. One reason A is not closed under multiplication. Take $a = a' = c = c' = 1$ and $b = b' = 0$. Then $g, g' \in A$ but $gg' \notin A$ as $b' + ac' + b = 1 \neq 0$.

(b) (**5 pts**) Let $g \in G$. Then $g \in \mathrm{C}_G(A)$ if and only if $gg' = g'g$ for all $g' \in A$ if and only if

$$\forall \;\; a', b'c' \in \mathbf{R}, a' = c' \;\text{ and }\; b' = 0 \;\text{ implies }\; ac' = a'c \tag{4}$$

Suppose (4) holds. Then taking $a' = c' = 1$ and $b' = 0$ we conclude $a = c$. If $a = c$ then (4) holds. Therefore $\mathrm{C}_G(A) = \{\begin{pmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix} \mid a, b \in \mathbf{R}\}$.

Comment: Careful with the quantifiers. The conclusion $a = c$ should be justified by a specific choice of numbers.

(c) (**5 pts**) Suppose $g \in \mathrm{N}_G(A)$. Then for $g' \in A$ there exists a $g'' \in A$ such that $g'g = g''g$ as $gA = Ag$. In terms of matrix entries: for all $a', b', c' \in \mathbf{R}$ such that $a' = c'$ and $b' = 0$ there exist $a'', b'', c'' \in \mathbf{R}$ such that $a'' = c''$ and $b'' = 0$ imply the equations

$$a + a' = a'' + a, \qquad b' + ac' + b = b + a''c + b'', \qquad c' + c = c + c'',$$

or equivalently

$$a' = a'', \qquad ac' = a''c, \qquad c' = c'',$$

or equivalently

$$a' = a'', \qquad ac' = c'c, \qquad c' = c'',$$

hold. (Why?) Thus with $a' = c' = 1$ and $b' = 0$ we conclude $a = c$. Therefore $g \in \mathrm{C}_G(A)$. We have shown $\mathrm{N}_G(A) \subseteq \mathrm{C}_G(A)$. Since $\mathrm{C}_G(A) \subseteq \mathrm{G}_G(A)$ holds generally, $\mathrm{N}_G(A) = \mathrm{C}_G(A)$.

(d) (**5 pts**) The set of part (d) is a subgroup of G since it is a centralizer which is always a subgroup of G.

5. (**20 points**) We use results from "Section 2.3 Supplement" on the course web page.

(a) (**5 pts**) The number of subgroups of G is the number of positive divisors of $|G| = 33 = 3{\cdot}11$. Thus there are 4.

(b) (**5 pts**) Since $<a^{-91}> = <a^{91}> = <a^{(33,91)}> = <a^{(3\cdot 11, 7\cdot 13)}> = <a^1> = <a>$ it follows that $|a^{-91}| = |<a^{-91}>| = |<a>| = |a| = 33$.

(c) (**5 pts**) a^ℓ is a generator if and only if $(\ell, 33) = 1$. Thus our list consists of multiples of each of the prime factors of 33, where $0 \le \ell < 33$. The list is

$$0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30; 11, 22.$$

(d) (**5 pts**) $<a^{12}> = <a^{(12,33)}> = <a^3>$ which has elements

$$e = a^0, a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}, a^{24}, a^{27}, a^{30}.$$